Modern Algebra

Mathematics degree honours course

Dr. Arnab Chakraborty

Assistant Professor
Indian Statistical Institute, Kolkata

Formerly

Guest Faculty
Ramakrishna Mission Vidyamandira, Belur

◇

Guest Faculty
Ramakrishna Vivekananda University, Belur

◇

Assistant Professor
St. Xavier's College, Kolkata

Sarat Book Distributors
18-B, Shyamacharan De Street
Kolkata 700 073

সূচী

III. Group theory (year 2) 177

ছাত্রছাত্রীদের প্রতি

এসে গেল Modern Algebra-র দ্বিতীয় সংস্করণ। প্রথম সংস্করণের পরে তোমরা অনেকে নানারকম পরামর্শ, অনুরোধ, অভিযোগ করেছিলে। সেইসব মাথায় রেখে বইটার খোলনলচে অনেকটাই বদলে ফেলেছি। যারা যারা নানারকম মতামত দিয়ে সাহায্য করেছ, তাদের সকলের তো নাম জানি না, তাই এখানে উল্লেখ করতে পারছি না। কিন্তু বিশেষভাবে যে দুজনের মন্তব্যের ভিত্তিতে বইটার অনেকটাই রদবদল করেছি তাঁরা হলেন শ্রীকল্লোল মাইতি আর শ্রীআবীরলাল সরকার। এঁদেরকে (এবং নাম-না-বলা শুভার্থীদেরকেও) অনেক অনেক ধন্যবাদ।
যারা আমাদের "বাংলায় বোঝানো ইংরাজী বই" সিরিজটা নতুন দেখছ, তাদের জানিয়ে রাখি যে, এই সিরিজটা লেখা হচ্ছে সেই সব ছাত্রছাত্রীদের কথা মাথায় রেখে যারা ইংরাজী মাধ্যমে পড়ছে, কিন্তু ইংরাজীর চেয়ে যাদের বাংলা বুঝতে বেশী সুবিধা হয়। এখানে যাবতীয় technical term ইত্যাদি ইংরাজীতেই লেখা, উত্তরগুলোও তাই। শুধু বোঝানো অংশটুকু বাংলায়।

যাদের ইংরাজী বুঝতে অসুবিধা হয় না, তারাও অনেক সময়ে বুঝতে পারো না যে, একটা অংকের উত্তর কি করে ইংরাজীতে লিখতে হয়। অংক লেখার ইংরাজী আর সাধারণ ইংরাজী ঠিক এক জিনিস নয়। কি করে একটা উত্তর ইংরাজীতে গুছিয়ে লিখতে হয় সেটা এই বইতে handwriting-এর মত লিখে দেখানো আছে।

বইটায় প্রচুর ছবি দেওয়া আছে। একটা অংকের উত্তর জানা থাকলে লিখে ফেলা কঠিন নয়। কঠিন হল উত্তরটা নিজে নিজে ভেবে বার করা। ছবিগুলো এই কাজে অপরিহার্য। এই বইয়ের অন্যতম উদ্দেশ্য হল তোমাকে ছবি এঁকে অংক করতে উৎসাহিত করা। অংক করার সময়ে যত পারবে ছবি আঁকবে, এমন কি পরীক্ষার খাতাতেও। ওতে সময় নষ্ট হয় না, বরং সময় বাঁচে।

বইটায় পাঁচটা অধ্যায় আছে। প্রথম দুটো first year-এর জন্য, তার পরের দুটো second year-এর জন্য, এবং শেষ অধ্যায়টা third year-এর জন্য। প্রতিটা অধ্যায়কে আবার day1, day2,... এইভাবে দিনে দিনে ভাগ করা আছে। মোটামুটিভাবে এক দিনের কাজ বলে যতটা দিয়েছি, সেটা হল কোচিং ক্লাসের দুই ঘন্টার পড়া। যেগুলো ইংরাজীতে লেখা সেগুলো যেন মাষ্টারমশাই বোর্ডে লেখাচ্ছেন, আর বাংলাগুলো মুখে বলছেন।

10 years' questions

যখন যে অধ্যায়টা শিখলে তখন তখনই সেই অধ্যায়ের 10 years' question-গুলো কষে ফেলা বুদ্ধিমানের কাজ। ঠিক এই নীতিতেই এই বইটা লেখা। প্রতিটি অধ্যায়ে সেই বিষয়ের দশ বছরের প্রশ্নগুলোর বিশদ উত্তর আলোচনা করা আছে। এমন কি ভুল অংকগুলোও বাদ নেই, সেগুলো কেন ভুল সেটাও বোঝানো আছে।

এই বইয়ের 10 years' question-গুলো নিয়েছি বাজারে প্রচলিত সংকলনগুলো থেকে। সুতরাং ভুল প্রশ্নগুলোর ভুলের দায় কতটা প্রশ্নকর্তার আর কতটা সংকলনকারীর সেটা জানি না। এই বইটাকে যথাসম্ভব ত্রুটিমুক্ত রাখতে চেষ্টা করেছি। তাও কিছু ভুল থেকে যাওয়া অসম্ভব নয়। কোনো ভুলের সন্ধান পেলে, বা অন্য কারণে যোগাযোগ করতে চাইলে email (arnabc74@gmail.com) বা ফোন (9231542600) ব্যবহার করতে পারো। আর এই webpage-টায় চোখ রেখো--

`http://www.isical.ac.in/~arnabc/modalged2`

এই বইয়ের ভুলত্রুটিগুলো বেরোলে ওখানে বলে দেব। আর তোমার মন্তব্য লেখারও একটা জায়গা আছে ওখানে।

অর্ণব চক্রবর্তী

Chapter I
Set, relation, function (year 1)

DAY 1
একেবারে গোড়ার কথা

এই বইয়ের বিষয়বস্তু হল modern algebra. এর মধ্যে algebra জিনিসটা কী, তার সঙ্গে তো স্কুলে থাকতেই তোমার ভালো রকম পরিচয় হয়েছে। সুতরাং modern algebra নাম শুনেই নিশ্চয়ই ভাবছ যে, আমরা algebra-র কোনো সদ্য আবিষ্কৃত আধুনিক সংস্করণ দিয়ে আলোচনা শুরু করব। মজার কথা হল আমরা তার ঠিক উল্টোটা দিয়ে আরম্ভ করব! আমরা শুরু করব অংকের দুনিয়ার প্রাচীনতম জিনিস নিয়ে--সেই সব জিনিস যেগুলো সভ্যতার আদি থেকে, বা তারও আগে থেকে মানুষ জানত। সেই জিনিস যেটা একটা ছোটো বাচ্চা, কিংবা নিতান্ত অশিক্ষিত মানুষও স্বচ্ছন্দে বুঝতে পারে। যা না বুঝলে আমাদের পক্ষে প্রতিদিনের জীবনে বেঁচে থাকাই অসম্ভব হত, আমাদের প্রথম বিষয়বস্তু হবে সেটা। কি সেই জিনিস?
আচ্ছা, তুমি তো স্কুলে অনেক রকম অংকটংক শিখে এসেছো, তুমি বলো তো অংকের জগতের সবচেয়ে সহজ জিনিস কী? যেটা একেবারে গোড়ার জিনিস? যেটা বুঝতে আগেভাগে আর কিচ্ছু জানার প্রয়োজন পড়ে না?
তুমি হয় তো উত্তর দেবে--$1, 2, 3, \ldots$ ইত্যাদি গুণতে পারা, বা ছোটোখাটো যোগ বিয়োগ করা, ইত্যাদি। কিন্তু না, এগুলো মানব সভ্যতায় এসেছে বহু পরে। গোড়ায় কী ছিল সেটা বোঝার জন্য একটা উদাহরণ দেখি।

Example 1: Fig 1-এর দিকে তাকাও। বল তো এখানে কতগুলো ছেলে আর কতগুলো মেয়ের ছবি রয়েছে? তুমি চোখে

দেখেই উত্তর দেবে--4-টে ছেলে আর 2-টো মেয়ে। একটা বাচ্চাকে একই প্রশ্ন কর, সে হয় তো চোখে দেখে বলতে পারবে না, আঙুল দিয়ে গুণে গুণে বলবে। কিন্তু আমাদের দেশে এমন বহু অশিক্ষিত লোক আছে যারা এই গোণাটুকুও করতে পারবে না! শুনতে যতই আশ্চর্য লাগুক, সভ্যতার আদিতে সব মানুষই এই অবস্থায় ছিল। কারণ সংখ্যার ধারণাই তখনও আবিষ্কারই হয়নি! ■

তাহলে অংক জিনিসটার শুরুটা হল কী করে? সেটা বোঝার জন্য প্রশ্নটাকে একটু পাল্টানো যাক। এবার কাজ হল যাবতীয় ছেলেদেরকে একটা লাইন টেনে গোল করে ঘিরে দিতে হবে, আর মেয়েদেরকেও আরেকটা গোল করে ঘিরে দিতে হবে (Fig 2)। এই কাজটা কিন্তু সবাই পারবে, বাচ্চাবুড়ো, শিক্ষিত, অশিক্ষিত সবাই। কারণ এর জন্য খালি ছেলেগুলোকে ছেলে এবং মেয়েগুলোকে মেয়ে বলে চিনতে পারাই যথেষ্ট। বুঝতেই পারছ এটা গুণতে শেখারও অনেক আগের জিনিস, যদি কে ছেলে আর কে মেয়ে সেটা চিনতেই না পারো, তবে আর ওদের গুণবে কী করে?

Fig 1

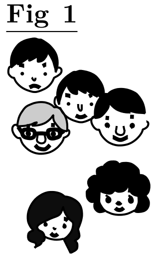
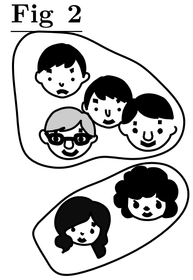


Fig 2



এই যে ছেলেগুলোকে গোল করে ঘিরে দিতে বললাম, সেটাকেই বলব ছেলেদের **set.** এক গুচ্ছ একইরকম জিনিস দেখলেই মানুষের মন চট্ করে তাদের সাদৃশ্যটুকু খুঁজে নিয়ে মনে মনে একটা set বানিয়ে ফেলে। যেমন ধরো, তুমি একটা বাচ্চাকে বোঝানোর চেষ্টা করছ "লাল রং" কাকে বলে। তার জন্য তুমি প্রথমে তাকে অনেকগুলো লাল রঙের জিনিস দেখাবে--একটা লাল বল, লাল জামা, লাল গোলাপ, ইত্যাদি। আর মুখে বার বার করে "লাল" শব্দটা বলবে। বাচ্চাটা অমনি মানুষের স্বভাব-ধর্ম অনুসারে অনুধাবন করবে যে বল, জামা এবং গোলাপ এই তিনটেরই মধ্যে যে বৈশিষ্ট্যটা common, সেটার নামই নিশ্চয়ই "লাল"। অর্থাৎ বাচ্চাটা মনে মনে ওই বল, জামা এবং গোলাপের মধ্যে common বৈশিষ্ট্যটা বুঝে নিয়ে ওই বৈশিষ্ট্যওয়ালা সব জিনিসকে ঘিরে একটা গোল এঁকে নিল, এবং এই set-টার নাম ওর মগজে চিরতরে আঁকা হয়ে গেল--"লাল"। একটু চিন্তা করলেই দেখবে যে, আমাদের মনে থরে থরে এরকম প্রচুর set সাজানো আছে--

- "আমি একটা ছেলে" মানে "আমি ছেলেদের set-এর মধ্যে আছি।"
- কলেজের প্রিন্সিপাল জানতে চেয়েছেন "সুরঞ্জনা বসু কোন ক্লাসে পড়ে?" রেজিস্ট্রার জাবদা খাতা খুলে খুঁজে দেখছেন। সেই খাতায় কী আছে? আছে অনেকগুলো set-এর হদিস, কারণ প্রতিটা ক্লাসের যাবতীয় ছাত্র নিয়ে একেকটা set হয়। "সুরঞ্জনা বসু" এদের মধ্যে কোন set-এ আছে সেটাই প্রশ্ন।

এখন কথা হল set যদি এত প্রাচীনকালের জিনিসই হবে, তবে তা নিয়ে modern algebra-র বইতে মাথা ঘামাচ্ছি কেন? কারণ প্রাচীনকাল থেকে মানুষ এইসব ধারণা ব্যবহার করে এসেছে বটে, কিন্তু সেটা সচেতনভাবে নয়। এই সচেতনতাটা নিতান্তই আধুনিক কালে এসেছে। যেমন গুহামানবরাও নিঃশ্বাসের সময়ে অক্সিজেন নিত, কিন্তু অক্সিজেন পদার্থটা কী, সেটা বুঝতে আরো অনেক সময় লেগেছিল। কোনো বিষয়ে সচেতনতা এলেই সেটা প্রকাশ করতে নতুন কিছু notation-এর জন্ম হয়। Set-এর বেলাতেও তার অন্যথা হয় নি। এই notation-গুলো কিছুটা তোমরা স্কুলে থাকতেই দেখেছো। একটু মনে করে নেওয়া যাক।

1.1 $\subseteq, \cup, \cap$

- সাধারণতঃ set-দেরকে ইংরাজী বড়হাতের অক্ষর দিয়ে নাম দেওয়া হয়। Set-এর সদস্যদের বলে একেকটা **element,** যাদের সাধারণতঃ ছোটোহাতের অক্ষর দিয়ে লেখা হয়। যেমন $A = \{1, 3, 5\}$-এর মধ্যে একটা element হল $x = 3$.
- অনেক সময়ে আমরা এমন set নিয়ে কাজ করি যার element-গুলোও একেকটা set. এরকম ক্ষেত্রে মূল set-টাকে লোকে script অক্ষর (মানে হাতের লেখার মত প্যাঁচানো অক্ষর) দিয়ে লেখে (যেমন $\mathcal{A}, \mathcal{B}, \mathcal{C}$), আর element-গুলোকে লেখে বড়হাতের অক্ষর দিয়ে। যেমন

  $$\mathcal{D} = \{ \ \{1, 2\}, \quad \{1\}, \quad \{3, 4, 5\} \ \}$$

  হলে তার একটা element হল $A = \{1, 2\}$.
- যদি কোনো জিনিস কোনো একটা set-এর element হয়, সেই ব্যাপারটা $\in$ বা **belongs to** চিহ্ন দিয়ে বোঝানো হয়। যেমন এক্ষুণি যে $\mathcal{D}$-টা দিলাম তার জন্য আমরা বলতে পারি

  $$\{1, 2\} \in \mathcal{D}.$$

  কিন্তু $\{2\}$ মোটেই $\mathcal{D}$-এর element নয়, তাই লিখব

  $$\{2\} \notin \mathcal{D}.$$
- অংক কষার সময়ে ছবি এঁকে নিলে সুবিধা হয়। Set-এর ছবি আঁকার একটা কায়দা হল **Venn diagram** (ভেন্ ডায়াগ্রাম)। এখানে set-গুলোকে গোল চৌকো ইত্যাদি বিভিন্ন আকারের ঘেরা জায়গার মত করে দেখানো হয়। একটা উদাহরণ রয়েছে Fig 3-এ।
- **Subset:** একটা set A যদি আরেকটা set B-র পেটের মধ্যে থাকে তবে আমরা A-কে বলি B-র **subset,** আর B-কে বলি A-র **superset.** ছবিতে দেখিয়েছি Fig 4-এ।

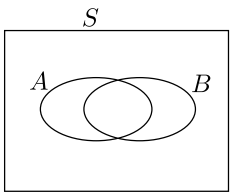


Fig 3

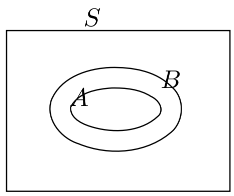


Fig 4

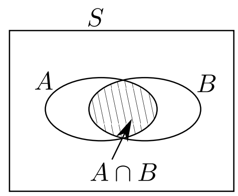


Fig 5

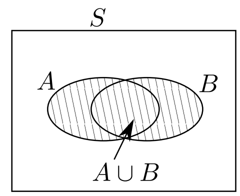


Fig 6

- **Intersection:** যদি A, B দুটো set হয়, তবে যেসব element এদের দুজনের মধ্যেই আছে তাদের set-টাকে লেখে $A \cap B$, যেটাকে মুখে বলে A **intersection** B. যেমন A যদি হয় মেয়েদের set আর B যদি হয় চশমা-পরাদের set, তবে $A \cap B$ হল চশমা-পরা মেয়েদের set. ছবি দ্যাখো Fig 5-এ।

- **Union:** যদি A, B দুটো set হয়, তবে যে সব element A বা B-এর অন্ততঃ একটাতে আছে, তাদের set-কে লেখে লেখে $A \cup B$, আর মুখে বলে A **union** B. ছবি রয়েছে Fig 6-এ। একটা মিশন-পরিচালিত কলেজে ভর্তির ব্যাপারে নিয়ম দেওয়া আছে এইরকম--যারা হায়ার সেকণ্ডারীতে অংকে অন্ততঃ 60% পাবে তারা ভর্তি হতে পারবে। আর যদি তুমি সেই মিশনের পরিচালিত স্কুল থেকে পাশ করে থাকো তাহলে তুমি এমনিই ভর্তি হতে পারবে। যদি A হয় হায়ার সেকণ্ডারীতে $\geq 60\%$ নম্বর পাওয়াদের set, আর B হয় মিশনের স্কুল থেকে পাশ করাদের set, তবে ভর্তি হবার জন্য তোমাকে হয় A অথবা B-র element হতে হবে। অর্থাৎ ভর্তি হতে পারবে $A \cup B$-এর সদস্যরা।

- **Set minus:** ধরো A, B হল দুটো set. তাহলে $A \setminus B$ হল সেই সব element-দের set যারা A-তে আছে কিন্তু B-তে নেই (Fig 7)। যেমন $A = \{1, 2, 3\}$ আর $B = \{2, 4, 6\}$ হলে $A \setminus B = \{1, 3\}$. মুখে বলার সময়ে $A \setminus B$-কে বলি A **set-minus** B. অনেক সময়ে লোকে এটাকে $A - B$-ও লেখে, যদিও সেটা না লেখাই ভালো, কারণ সাধারণ সংখ্যার বিয়োগের সঙ্গে গুলিয়ে যেতে পারে।

- **Universal set:** একটা চশমার দোকানের বাইরে মাইক বাজিয়ে বিজ্ঞাপন দেওয়া হচ্ছিল--দূরের লেখা যারা পড়তে পারেন না, তারা আমাদের চশমা ব্যবহার করলেই অনায়াসে দূরের লেখা পড়তে পারবেন। তাই শুনে একজন অশিক্ষিত লোক দৌড়ে এল চশমা করাতে, সে আদৌ পড়তেই জানে না, বিজ্ঞাপন শুনে তার বিশ্বাস হয়েছে যে, সেই আশ্চর্য চশমা নাকে ঝোলালেই সে পড়তে শিখে যাবে! যদি S হয় সব পড়তে জানা লোকের set, আর A হয় সেই সব লোকের set যারা দূরের লেখা পড়তে পারে, তাহলে চশমাটা হল $S \setminus A$-র জন্য। সুতরাং খুব আইন বাঁচিয়ে বলতে হলে বিজ্ঞাপনটার বয়ান হওয়া উচিত ছিল--যারা পড়তে জানেন, অথচ দূরের লেখা পড়তে পারেন না, তারা আমাদের চশমা পরলে উপকৃত হবেন। বলাই বাহুল্য যে এত আইন বাঁচিয়ে কেউ বিজ্ঞাপন দেয় না। কারণ নিতান্ত গবেট ছাড়া সকলেই বুঝবে যে, এখানে কথাটা হচ্ছে কেবলমাত্র পড়তে জানা লোকেদের নিয়েই। অংকের জগতেও এই কায়দাটা চলে। যদি আমাদের আলোচনা কোনো একটা বিশেষ set-এর element-দের মধ্যেই সীমাবদ্ধ থাকে, তবে সেই set-টাকে বলে সেই আলোচনার **universal set.** চশমার উদাহরণে যেমন যাবতীয় পড়াশোনা-জানা লোকের set S ছিল universal set.

- **Complement:** যদি S হয় universal set, তবে $S \setminus A$-কে সংক্ষেপে লেখে A^c, (যাকে বলে A **complement**). Fig 8 দেখে এই ব্যাপারটা একটু ভালো করে বুঝে নাও। A^c চিহ্নটার মধ্যে S-এর কোনোই উল্লেখ নেই, কিন্তু ওটার মধ্যে S-টা লুকিয়ে ঢুকে আছে, S বদলালে A^c-এর অর্থ বদলে যাবে! যেমন যদি S হয় যাবতীয়

Fig 7

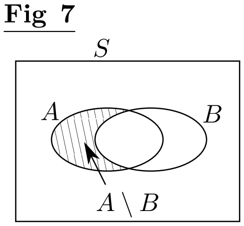
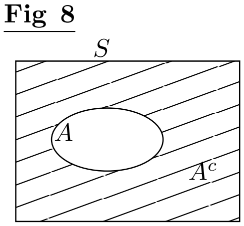


Fig 8



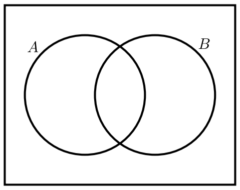


Fig 9

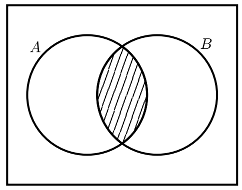


Fig 10

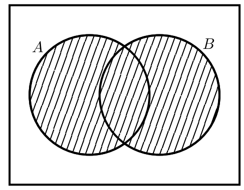


Fig 11

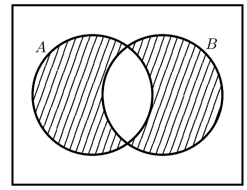


Fig 12

integer-এর set, আর A হয় যাবতীয় even (জোড়) সংখ্যার set, তবে A^c হবে যাবতীয় odd (বিজোড়) সংখ্যার set. কিন্তু যদি S হত যাবতীয় real number-এর set, তবে কিন্তু A^c-এর মধ্যে $\frac{1}{2}$-ও থাকত।

1.2 চোখ, বাইনোকুলার, চাঁদ আর পরোটা

কিছু set মিলিয়ে মিশিয়ে কোনো ফর্মুলা দিলে সেটাকে Venn diagram দিয়ে এঁকে ফেলতে অনেকেই পারে (যেমন আমরা এক্ষুণি আঁকলাম), কিন্তু Venn diagram থেকে ফর্মুলায় পৌঁছতে অনেক ছাত্রকেই নাজেহাল হতে দেখি। সেই কাজটায় একটু সড়গড় হয়ে নেওয়া যাক। ধরো দুটো set আছে A, B, যেমন দেখিয়েছি Fig 9-এ।

Exercise 1: মাঝখানে চোখের মত set-টার ফর্মুলা আমরা এক্ষুণি শিখলাম (Fig 10)। বলো তো কী? ■

Exercise 2: সিনেমায় যেমন বাইনোকুলার দিয়ে দেখা বোঝায়, সেরকম একটা set হয়েছে Fig 11-এ। এটার ফর্মুলাও একটু আগেই বললাম। কী বলো তো? ■

Exercise 3: Fig 12-এ দু পাশে দুটো চাঁদের মত ঠেলে বেরিয়ে আছে দেখেছো? বাঁদিকের চাঁদটার ফর্মুলা কী হবে? আর ডান দিকের চাঁদটার? ■

যদি দুটো চাঁদকে একসঙ্গে নাও, তবে যে set-টা পাবে তাকে বলে A আর B-এর **symmetric difference,** আর লেখে $A\Delta B$. একটু চিন্তা করলেই বুঝবে যে $A\Delta B = B\Delta A$. বস্তুতঃ সেই জন্যেই "symmetric" বলা হয়।

Exercise 4: $A\Delta B$-কে কেবলমাত্র union, intersection আর complement ব্যবহার করে লিখতে পারবে? ■

Exercise 5: সবকিছুর বাইরে যে আকাশের মত যে set-টা (Fig 13), ওটার ফর্মুলা কী হবে? ■
ওটা

এই তো গেল দুটো set দিয়ে আঁকা Venn diagram-এর কথা। যদি তিনটে set থাকে (Fig 14-এর মত) তবে বৈচিত্র্য আরও বাড়বে। Fig 15-এ কতগুলো টুকরো রয়েছে দেখেছো? এই আটটা টুকরোর প্রত্যেকের ফর্মুলা বার করার খুব সহজ

Fig 13

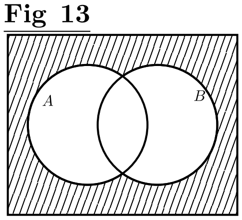


Fig 14

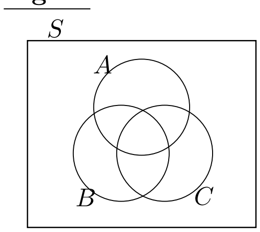
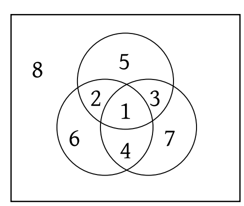


Fig 15



আহ্লাদে আটখানা!

কায়দা আছে। যেই তোমাকে একটা টুকরো দিয়ে তার ফর্মুলা বার করতে বলবে অমনি তুমি প্রথমে $A\cap B\cap C$ লিখে শুরু করবে। তারপর দেখবে টুকরোটা A,B আর C-এর কাদের কাদের মধ্যে নেই। তাদের ক্ষেত্রে একটা করে complement বসিয়ে দেবে। দুটো উদাহরণ দেখি।

Example 2: মাঝখানে একটা পরোটা দেখছো (1 নম্বর টুকরো)? ওটার ফর্মুলা কি হবে?

SOLUTION: শুরু করি $A\cap B\cap C$ লিখে। পরোটাটা A,B,C তিনজনের মধ্যেই রয়েছে, সুতরাং কোনো complement লাগবে না। অতএব উত্তর হল $A\cap B\cap C$. ■

Example 3: দুর্গাঠাকুরের প্রতিমায় কপালে একটা চোখ আঁকে। আমাদের Venn diagram-এও সেরকম একটা খাড়া চোখ আছে। সেটা থেকে পরোটাটাকে বাদ দিলে পড়ে থাকে যে টুকরোটা সেটাকে Fig 15-এ 4 নম্বর টুকরো বলেছি। এর ফর্মুলা কি হবে?

SOLUTION: শুরু করব যথারীতি $A\cap B\cap C$ লিখে। এবার দ্যাখো যে, টুকরোটা A-এর মধ্যে নেই, কিন্তু B আর C-এর মধ্যে আছে। সুতরাং A-এর complement নিয়ে উত্তর হবে $A^c\cap B\cap C$. অবশ্য এই টুকরোটাকে তুমি "চোখ থেকে পরোটা বাদ" বলেও লিখতে পারতে--$(B\cap C)\setminus(A\cap B\cap C)$. ■

Exercise 6: আটটা টুকরোর প্রত্যেকটার জন্য ফর্মুলাগুলো লিখে ফ্যালো। ■

1.3 Set-builder notation

অনেক সময়ে আমরা একটা set-এর সঙ্গে সম্পর্ক দিয়ে আরেকটা set তৈরী করি। আমার বাড়ির কাছে একটা বাচ্চাদের স্কুল আছে। প্রতিদিন কাজে যাবার পথে দেখি তার সামনে প্রচুর ভদ্রমহিলার ভীড়। এঁরা কারা? স্কুল-পড়ুয়াদের মায়েরা। অর্থাৎ এই ভদ্রমহিলাদের set-টাকে আমরা প্রকাশ করছি আরেকটা set-এর সঙ্গে সম্পর্ক দিয়ে--স্কুল-পড়ুয়াদের set. যদি স্কুলের বাচ্চাদের set-টাকে S নাম দিই, তবে মায়েদের set-টাকে অংকের ভাষায় লিখব--

$$\{x\text{-এর মা} \ : \ x\in S\}.$$

এটাকে পড়ব এইভাবে-- x-এর মায়েদের set, যেখানে $x\in S$.
এইভাবে একটা set দিয়ে আরেকটা set-কে প্রকাশ করাকে বলে **setbuilder notation.** এটা অংকে বহুল ব্যবহৃত একটা notation.

Example 4: Setbuilder notation দিয়ে লেখো--

(1) যাবতীয় square number-এর set, **(2)** সেই সব সংখ্যার set যাদেরকে 3 দিয়ে ভাগ করলে ভাগশেষ হয় 2.
SOLUTION:
(1) $\{n^2 \ : \ n\in\mathbb{Z}\}$ **(2)** $\{3n+2 \ : \ n\in\mathbb{Z}\}$. ■

1.4 $\forall, \exists, \neg$

এবার আরো কিছু notation শিখব যেগুলো নতুন, স্কুলে এদের সঙ্গে পরিচয় হয় না।

- **For all** $(\forall)$: অনেক সময়ে আমরা এমন কোনো বৈশিষ্ট্যের কথা বলি যেটা একটা set-এর সব element-এরই আছে। যেমন ধরো বললাম যে--

  ওই মেসে যে ছেলেগুলো থাকে তারা সবাই মোহনবাগানের সাপোর্টার।

এখানে "মোহনবাগানের সাপোর্টার" একটা বৈশিষ্ট্য, যেটা মেসের ছেলেদের set-এর সব element-এর ক্ষেত্রেই প্রযোজ্য। এটাকে অংকের ভাষায় লেখার জন্য ওই মেসের যাবতীয় ছেলের set-টার একটা নাম দিয়ে নেব, ধরো M. তাহলে লিখতে পারি--

$$\forall x \in M \quad x \text{ supports Mohanbagan.}$$

এটাকে পড়ব--"For all x in M, x supports Mohanbagan."

- **There exists** ($\exists$) : সৈকতদের বাড়িতে একরাশ বেড়াল আছে। তাদের নিয়ে সারা পাড়া অতিষ্ঠ। পাশের বাড়ির রান্নাঘরে এক বাটি দুধ ছিল, কোনো একটা বেড়াল এসে চুপিসাড়ে খেয়ে গেছে। সে বাড়ির বৌ ক্ষেপে গিয়ে বলছে এটা নির্ঘাত সৈকতদের বাড়ির বেড়ালগুলোর কাজ। সে বাড়ির বৌ অবশ্য অংকের ভাষার ধার ধারে না, কিন্তু আমরা কি তার অভিযোগটাকে এইভাবে লিখলে ঠিক হবে? (ধরো S হল সৈকতদের বাড়ির সব বেড়ালের set):

  $$\forall c \in S \quad c \text{ has stolen milk.}$$

  না হবে না, কারণ এতে মনে হচ্ছে যেন সৈকতদের বাড়ির সবগুলো বেড়াল মিলে দুধটা খেয়েছে। আসলে অভিযোগটা হল--অন্ততঃ একটা বেড়াল এসে অপকর্মটা করে গেছে। এরকম "অন্ততঃ একটা" বোঝানোর জন্য $\forall$ চলবে না, ওর জন্য একটা আলাদা notation আছে--$\exists$ বা there exists. সেটা ব্যবহার করে লিখতে পারি--

  $$\exists c \in S \quad c \text{ has stolen milk.}$$

  এটাকে পড়ব--"There exists a c in S such that c has stolen milk. লক্ষ করো যে "such that" কথাটা লেখা ছিল না, কিন্তু $\exists$ থাকলেই পড়ার সময়ে আমরা একটা "such that" জুড়ে নিই।

- **Not** বা **negation** ($\neg$) : সৈকতের দিদি আবার পাশের বাড়ির বৌটাকে দু'চক্ষে দেখতে পারে না। সুতরাং পাশের বাড়ির বৌ যাই বলুক সৈকতের দিদি তার উল্টোটা বলবেই। অংকের জগতে অবশ্য এরকম চুলোচুলি হয় না, কিন্তু তাও মাঝেমাঝেই আমাদেরকে কোনো বাক্যের বিপরীতার্থক বাক্য গঠন করতে হয়। তার জন্য প্রধান অস্ত্র হল $\neg$ বা negation. সেটা ব্যবহার করলে সৈকতের দিদির বক্তব্যটা দাঁড়াবে--

  $$\neg(\text{পাশের বাড়ির বৌয়ের বক্তব্য}).$$

  মানে

  $$\neg(\exists c \in S \quad c \text{ has stolen milk}).$$

1.5 অংকের ব্যাকরণ

আমরা তিনটে নতুন চিহ্ন শিখলাম--$\forall, \exists$ আর $\neg$. অনেক সময়ে একই বাক্যে একাধিক চিহ্ন একসাথে ব্যবহার করতে হয়। এর একটা উদাহরণ আমরা ইতিমধ্যেই দেখেছি--সৈকতের দিদির বক্তব্যে--

$$\neg(\exists c \in S \quad c \text{ has stolen milk}).$$

এখানে একই বাক্যে $\neg$-ও আছে, আবার $\exists$-ও আছে। আরেকটা উদাহরণ এইরকম হতে পারে-- যদি বলি "সৈকতদের বন্ধুরা সবাই ওদের বাড়ির সব বেড়ালকে ভালোবাসে" তবে সেটা অংকের ভাষায় হবে (সৈকতের যাবতীয় বন্ধুর set-টাকে F নাম দিলে)--

$$\forall f \in F \quad \forall c \in S \quad f \text{ loves } c.$$

এখানে একই বাক্যে দুটো $\forall$ ব্যবহার করেছি।
একই বাক্যে এরকম একাধিক চিহ্ন ব্যবহার করা নিয়ে অংকের ব্যাকরণে কয়েকটা সহজ কিন্তু গুরুত্বপূর্ণ নিয়ম আছে। সেগুলো শিখে রাখি--

1. পরপর দুই বা তার বেশী $\forall$ থাকলে তাদেরকে আগেপরে করলে বাক্যটার অর্থ বদলায় না। যেমন যদি বলি

   $$\forall c \in S \quad \forall f \in F \quad f \text{ loves } c.$$

   তার মানে হত সবগুলো বেড়ালকেই সব বন্ধুরা ভালোবাসে, যেটা একই কথা।

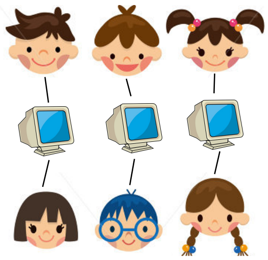


Fig 16

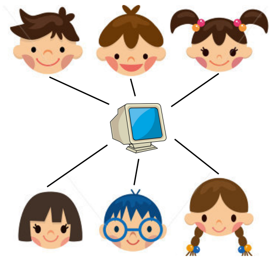


Fig 17

2. পরপর কিছু $\exists$-কেও আগেপরে করা যায় নিশ্চিন্তে, ওতেও বাক্যের অর্থ বদলাবে না।

3. কিন্তু যদি একটা $\forall$ আর একটা $\exists$ পরপর থাকে তবে কিন্তু ওদের আগেপরে করলে মানে বদলে যাবে। এটা নিয়ে অনেক ছাত্র ঝামেলায় পড়ে যায়। একটা উদাহরণ দেখি। সরকার থেকে কলেজে নির্দেশ এসেছে--

   সব ছাত্রকেই একটা কম্পিউটার ব্যবহার করতে দিতে হবে।

   এদিকে কলেজের বাজেট কম, তাই কলেজ কর্তৃপক্ষ করেছে কি ল্যাবে খালি একখানা কম্পিউটার কিনে সাজিয়ে রেখেছে। এদিকে ছাত্র অনেক। লম্বা লাইন, কেউই আর কম্পিউটার পায় না। আরো কম্পিউটার কেনার বিরুদ্ধে প্রিন্সিপালের মহান যুক্তি--আমরা তো সরকারের কথা অমান্য করতে পারি না! সব ছাত্রকেই একটা কম্পিউটার ব্যবহার করার নির্দেশ রয়েছে। আমরা কী করে আলাদা আলাদা ছাত্রের জন্য আলাদা আলাদা কম্পিউটার দিই?

   সাধারণ ভাষার মুস্কিল এই যে, কথার মারপ্যাঁচে দিনকে রাত করা যায়। কিন্তু অংকের ভাষায় লিখলেই কলেজের কারচুপি ধরা পড়ে যাবে। ধরো S হল সব ছাত্রের set, আর C হল সব কম্পিউটারের set. তাহলে সরকারের নির্দেশ ছিল (Fig 16)

   $$\forall x \in S \quad \exists c \in C \quad x \text{ can use } c.$$

   আর কলেজ কর্তৃপক্ষ মানে খাড়া করেছে (Fig 17)--

   $$\exists c \in C \quad \forall x \in S \quad x \text{ can use } c.$$

   এর মধ্যে দ্বিতীয়টা ঠিক হলে প্রথমটাও ঠিক হবে, কিন্তু প্রথমটা অনেক বেশী উদার, একটামাত্র কম্পিউটার দিয়ে যে সবাইকেই কাজ চালাতে হবে এমন কিছু জোর দিয়ে সেখানে বলা ছিল না। যেমন, Fig 16-র মত প্রতি দুজন ছাত্রপিছু একটা করে কম্পিউটার দিলেও সরকারী নির্দেশ কিছুমাত্র অমান্য হত না (এবং ছাত্ররাও বাঁচত!)।

4. যখনই অংকের ভাষায় কোনো বাক্য লিখবে, তখন যাবতীয় $\forall$ আর $\exists$ যেন বাক্যের গোড়ায় থাকে। অনেকেরেই বদভ্যাস থাকে (এমন কি অনেক ভালো বইতেও এই কাণ্ডটা করা থাকে) যে $\forall$-গুলোকে বাক্যের একেবারে শেষে পাঠিয়ে দেয়। এটা অংকের ব্যাকরণবিরুদ্ধ, এবং সেটা অতি সঙ্গত কারণেই। এক্ষুণি আমরা দেখলাম যে সরকারের নির্দেশ এবং কলেজ কর্তৃপক্ষের ব্যাখ্যা সমার্থক নয়। অথচ যদি $\forall$-টাকে বাক্যের শেষে পাঠিয়ে দাও তবে দুটোর মধ্যে পার্থক্য করার কোনো জো নেই, কারণ দুটোই হয়ে যাবে--

   $$\exists c \in C \quad x \text{ can use } c \quad \forall x \in S.$$

5. Negation-এর প্রভাবে $\forall$ হয়ে যায় $\exists$, আর $\exists$ হয়ে যায় $\forall$. সৈকতের দিদির সঙ্গে পাশের বাড়ির বৌয়ের ঝগড়া মনে আছে? সৈকতের দিদির বক্তব্য ছিল--

   $$\neg(\exists c \in S \quad c \text{ has stolen milk}).$$

   এবার ওই $\neg$-টাকে $\exists$-এর ডানদিকে নিয়ে যাও, এর ফলে $\exists$-টা উল্টে $\forall$ হয়ে যাবে--

   $$\forall c \in S \quad \neg(c \text{ has stolen milk}).$$

মানে

$$\forall c \in S \quad c \text{ has not stolen milk.}$$

এটা সৈকতের দিদির বক্তব্যটারই আরেকরূপ--আমাদের বাড়ির কোনো বেড়াল দুধ চুরি করে নি। কম্পিউটারের উদাহরণে এইভাবে বার করা যাক যে, ঠিক কী করলে সরকারের নির্দেশ অমান্য করা হত--

$$\neg(\forall x \in S \quad \exists c \in C \quad x \text{ can use } c),$$

তার মানে

$$\exists x \in S \quad \forall c \in C \quad x \text{ cannot use } c,$$

অর্থাৎ এমন একজন ছাত্র আছে যে বেচারী কোনো কম্পিউটারই পাচ্ছে না।

6. আমরা দেখেছি যে, একই বাক্যে একাধিক $\forall$ বা $\exists$ থাকতে পারে, এবং প্রত্যেকটা $\forall$ বা $\exists$-এর পরে একটা করে variable থাকে। খেয়াল রাখা দরকার যেন আলাদা আলাদা $\forall$ আর $\exists$-এর পরে আলাদা আলাদা variable লেখা হয়। যেমন যদি লিখি

$$\forall x \in A \quad \exists x \in B \quad x = x$$

তবে সেটা অংকের ব্যাকরণসম্মত হবে না, লেখা উচিত

$$\forall x \in A \quad \exists y \in B \quad x = y.$$

7. "কোনো square number কখনো prime হতে পারে না-- $1, 4, 9, 25$ ইত্যাদি।" (সাবধান 1 কিন্তু prime নয়!) এই কথাটাকে একজন ছাত্র অংকের ভাষায় লিখতে চেষ্টা করেছে এইভাবে--

$$\forall n^2 \in \mathbb{Z} \quad n^2 \text{ is not prime.}$$

এটা কিন্তু ঠিক লেখা হয় নি, কারণ কোনো $\forall$ বা $\exists$-এর পরে খালি একটা variable-ই বসতে পারে, কোনো ফর্মুলা নয়। এখানে n একটা variable, কিন্তু n^2 একটা ফর্মুলা। তাই এভাবে লিখলে ঠিক হত--

$$\forall n \in \mathbb{Z} \quad n^2 \text{ is not prime.}$$

1.6 প্রমাণ লেখার কায়দা

কোনো কিছুকে অংকের ভাষায় গুছিয়ে প্রমাণ করতে শেখাটা অত্যন্ত জরুরী। কী করে সেই কাজটা করতে হয় সেটা সংক্ষেপে শিখে রাখি। এই বিদ্যেটা সারাজীবন কাজে দেবে। কোনো কিছু প্রমাণ করার মোটামুটিভাবে দুটো কায়দা আছে--direct proof আর proof by contradiction. এদের নিয়ে একে একে আলোচনা করা যাক।

1.6.1 Direct proof

ধরো A, B দুটো set. আমরা কখন বলি যে $A \subseteq B$? যখন A-এর প্রতিটা element থাকে B-এর মধ্যে। এই কথাটাকে এইভাবে লিখতে পারি--

$$\forall a \in A \quad a \in B.$$

এটাই হল $A \subseteq B$-এর সংজ্ঞা। কখন বলব $A = B$? যদি একইসঙ্গে $A \subseteq B$ এবং $B \subseteq A$ হয়। এবার এই জিনিসটা কাজে লাগিয়ে একটা প্রমাণ করা যাক।

Example 5: Prove that $\{2m - 1 \ : \ m \in \mathbb{Z}\} = \{2m + 1 \ : \ m \in \mathbb{Z}\}$.

SOLUTION: প্রথমে set দুটোর নাম দিয়ে নিই--

> Let $A = \{2m - 1 \ : \ m \in \mathbb{Z}\}$ and $B = \{2m + 1 \ : \ m \in \mathbb{Z}\}$.

দুটো set-কে সমান দেখাবার প্রধান কায়দা হল কাজটাকে দুভাগে ভেঙে নেওয়া--$A \subseteq B$ এবং $B \subseteq A$. প্রথমে $A \subseteq B$ দেখানোর চেষ্টা করা যাক--

Step 1: Shall show $A \subseteq B$, ie,

$$\forall a \in A \quad a \in B,$$

সাবধান, এখানে যেন $\forall 2m-1 \in A \quad 2m-1 \in B$ লিখে ফেলো না। ওটা ভুল হবে কারণ $\forall$-এর পরে কোনো ফর্মুলা বসে না, খালি variable বসে। আমরা জানি যে $a \in B$ হওয়া মানে $a = 2m+1$ আকারে লিখতে পারা, সুতরাং--

ie,

$\forall a \in A \quad \exists m \in \mathbb{Z} \quad a = 2m+1.$

যেটা দেখাতে হবে সেটাকে প্রথমে এইভাবে $\forall, \exists$ ইত্যাদি দিয়ে একটা বাক্যে প্রকাশ করে নেওয়া খুব দরকার। অধিকাংশ ছাত্রই গোড়ায় এই কাজটা করে নেয় না বলে প্রমাণের মাঝখানে গিয়ে "ওই যাঃ কি যেন দেখানোর কথা ছিল?" বলে গুবলে যায়। আমাদের কাজ হল এই বাক্যটাকে প্রমাণ করা। এরকম যে কোনো বাক্যেরই শুরুতে কিছু $\forall, \exists$ ইত্যাদি থাকে, তার পর থাকে একটা শর্ত। এখানে শর্তটা হল $a = 2m+1$. পুরো ব্যাপারটাকে একটা খেলার মত মনে কর, যেটা দুজনের মধ্যে খেলা হচ্ছে। $\forall$-গুলো হচ্ছে তোমার প্রতিপক্ষের চাল, আর $\exists$-গুলো তোমার চাল। এখানে বাক্যটা শুরু হয়েছে একটা $\forall a \in A$ দিয়ে, তার মানে তোমার প্রতিপক্ষ প্রথমেই A-র যে কোনো একটা element a তোমার দিকে ছুঁড়ে দেবে--

$\boxed{\forall a}$ Take any $a \in A$.

বাঁদিকে ছোটো করে "$\forall a$" লিখেছি এইটা মনে করিয়ে দেবার জন্য যে আমরা বাক্যটার কত দূর এগিয়েছি। এরপর আছে একটা $\exists m \in \mathbb{Z}$. সুতরাং এবার তোমার চাল। তুমি প্রতিপক্ষের এই a-টা ব্যবহার করে একটা এমন $m \in \mathbb{Z}$ বানানোর চেষ্টা করবে যাতে বাক্যটার একেবারে শেষে যে শর্তটা আছে (মানে $a = 2m+1$) সেটা পালিত হয়। এর জন্য সব সময়ে একটু রাফ করে নেওয়া ভালো। এখানে a-র চেহারা হল $2n-1$ জাতীয়। আমাদের চাই $a = 2m+1$ হওয়া, সুতরাং $m = n-1$ নিলে কাজ হবে।

Then $a = 2n-1$ for some $n \in \mathbb{Z}$.

$\boxed{\exists m}$ Choose $m = n-1$.

ওই দ্যাখো, বাঁদিকে ছোট্টো করে "$\exists m$" লিখে নিয়েছি, যাতে খেয়াল থাকে বাক্যটার কতদূর অবধি এসেছি। আর কোনো $\forall$ বা $\exists$ নেই, তার মানে খেলা শেষ, এবার আম্পায়ার এসে পরীক্ষা করে দেখবেন যে, তোমার এবং তোমার প্রতিপক্ষের চালগুলো মিলে বাক্যের শেষের শর্তটা পালিত হয় কিনা। যদি হয় তবে তোমার জিত (মানে প্রমাণটা হল), যদি না হয়, তবে তোমার হার (মানে প্রমাণটা হল না)। এবার আম্পায়ারের কাজ শুরু হচ্ছে, সেটা বোঝাতে বাঁদিকে ছোটো করে 🔍 এঁকে নেব। এই বাঁদিকের ছোটো করে লেখাগুলো কিন্তু খালি তোমার সুবিধার জন্য, ওগুলো প্রমাণের অঙ্গ নয়।

🔍 Then $a = 2n-1 = 2(m+1)-1 = 2m+1$, as required.

ওই যে শেষে "as required" লিখলাম, ওতেই বোঝা যাচ্ছে যে Step 1-এ জয়টা তোমারই হয়েছে। এখনো কিন্তু অংকটা শেষ হয় নি। আমরা সবে দেখিয়েছি যে $A \subseteq B$. আমাদের এখনও দেখাতে হবে যে $B \subseteq A$.

Step 2: Shall show $B \subseteq A$.

এই প্রমাণটাও ঠিক আগেরটারই মতন। তাই আর করে দেব না। নিজে নিজে লেখার চেষ্টা কর দেখি! ■

এই যেভাবে প্রমাণটা করলাম এটাকে বলে direct proof. এরকম প্রমাণ শুরু হয় একটা target বাক্য নিয়ে, তার পর $\forall, \exists$ অনুযায়ী খেলাটা চলতে থাকে, সবশেষে শর্তটা মেলাতে হয়। এই বইয়ের অধিকাংশ প্রমাণই এই কায়দায় করা হয়েছে। কিন্তু কিছু কিছু ক্ষেত্রে direct proof করা কঠিন। সেরকম ক্ষেত্রে আমরা আরেকটা কায়দা ব্যবহার করি, তাকে বলে proof by contradiction, যেটা এবার আমরা আলোচনা করব।

1.6.2 Proof by contradiction

একটা উদাহরণ নিয়ে বোঝা যাক।

Example 6: আমাদের ক্লাসে দুটো ছেলে আছে, তারা দেখতে ভীষণ এক রকম! ওদের একজনের নাম কুনাল, অন্যজনের কুশল--কুনাল বসু আর কুশল নাগ। আচ্ছা, ওরা কি যমজ?

SOLUTION: তুমি প্রশ্নটা শুনেই বলবে--"সে আবার কী কথা, ওরা কী করে যমজ হয়, দেখাই যাচ্ছে একজন বসু, অন্যজন নাগ!" এই যে তুমি কথাটা বললে এর পিছনের যুক্তিটাকেই বলে proof by contradiction. তুমি প্রথমে এটা ধরে শুরু করলে যে, সত্যিই যমজ হলে কী হত। তবে ওরা অবশ্যই এক বাবা-মায়ের সন্তান হত, এবং সেক্ষেত্রে ওদের পদবী একই হত। কিন্তু দেখাই যাচ্ছে যে, ওদের পদবী আলাদা। অর্থাৎ যমজ হলে যা হত আর যা হয়েছে, এ দুয়ের মধ্যে একটা অসঙ্গতি রয়েছে। এই অসঙ্গতিকেই বলে contradiction বা পরস্পরবিরোধিতা। এই contradiction থেকেই সিদ্ধান্ত করতে পারছি যে, প্রথমে যেটা ধরে নিয়ে শুরু করেছিলাম (যে ওরা যমজ) সেটা ঠিক হতে পারে না। এরকম প্রমাণের মূল কাঠামোটা এইরকম--

> Let, if possible, the two boys be twins.

যে কোনো proof by contradiction শুরু হয় Let, if possible, দিয়ে। যেটা প্রমাণ করতে হবে তার উল্টোটা ধরে নিয়ে। এর পর নানা রকম ধাপ--

> $\therefore$ They must have same parents.
> $\therefore$ They must have same surname.

"Surname" মানে হল পদবী।

> But one of them has surname "Basu" and the other has surname "Nag"
> $(\Rightarrow\Leftarrow)$

এরকম প্রমাণের শেষে আমরা একটা contradiction-এর পৌঁছই, সেটা বোঝানোর চিহ্ন হল $\Rightarrow\Leftarrow$. যে কোনো proof by contradiction-ই শুরু হয় Let, if possible, দিয়ে আর শেষ হয় $\Rightarrow\Leftarrow$ দিয়ে। এরপর একটা উপসংহার লিখে দেওয়া যায়--

> So they cannot be twins.

■

একটা কিছু প্রমাণ করতে দিলে কী করে বোঝা যাবে যে, direct proof করা উচিত নাকি proof by contradiction? এক কথায় এর কোনো সহজ উত্তর নেই। অনেক অংকই দুই পথেই করা যায়। তবে মোটামুটিভাবে বোঝার কায়দাটা হল--প্রথমে direct proof করার চেষ্টা কর। যদি হয়ে গেল, ভালো, নাহলে proof by contradiction-এর পথে এগোও।

1.7 Vacuously true

অংকে অনেক সময়ে একটা কথা শুনবে--**vacuously true** (ভ্যাকুয়াসলি ট্রু)। এই জিনিসটা কী, সেটা একটা গল্প দিয়ে বুঝে নিই, কারণ এই বইতে ব্যাপারটা কয়েকবার কাজে লাগবে। মনে কর তোমার বিরুদ্ধে অভিযোগ এসেছে যে তুমি কাউকে

খুন করেছ (কি সাংঘাতিক!) তোমাকে আদালতে তোলা হয়েছে। তোমার উকিল অবশ্যই প্রাণপণে চেষ্টা করছেন তোমাকে নির্দোষ সাব্যস্ত করতে। কিন্তু দুঃখের বিষয়, তোমার স্বপক্ষে কোনোই প্রমাণ পাওয়া যাচ্ছে না। তবে মজার কথা হল, বিপক্ষের হাতেও কোনো প্রমাণ নেই যে তুমিই খুনটা করেছ। সুতরাং তোমার নির্দোষিতার স্বপক্ষে যেমন কোনো প্রমাণ নেই, তেমনি বিরুদ্ধেও প্রমাণ দেওয়া যাচ্ছে না। এরকম কাণ্ড আদালতে আকছারই হয়ে থাকে, এবং এরকম অবস্থা সামাল দিতে অধিকাংশ দেশেই একটা নিয়ম আছে--benefit of doubt, এর মানে হল যদি কোনো পক্ষেই উপযুক্ত প্রমাণ না থাকে তবে প্রমাণাভাবে আসামীকে নিরপরাধ ধরা হবে। (সাবধান, সব দেশেই কিন্তু এই নিয়ম নয়। শুনেছি নেপালের নিয়ম ঠিক উল্টো। সুতরাং নেপালে গিয়ে ফেঁসে গেলে যেন আমায় দোষ দিও না!) নেপালে যাই থাক, অংকের জগতে কিন্তু benefit of doubt প্রচলিত, এবং এখান থেকেই vacuously true ব্যাপারটা আসে। একটা উদাহরণ দিই। আমরা জানি যে $A\subseteq B$ মানে

$$\forall x\in A\quad x\in B.$$

এ থেকে বল তো $\phi\subseteq\{1,2\}$ এই বাক্যটা ঠিক না ভুল? মনে রেখো, অংকের জগতে কিন্তু সব কিছুই ঠিক অথবা ভুল, মাঝামাঝি কিছু হয় না! আমাদের বাক্যটাকে বিশদ করে লিখলে হয়

$$\forall x\in\phi\quad x\in\{1,2\}.$$

সমস্যা হল ϕ-এর মধ্যে তো কোনো x নেওয়াই অসম্ভব! অর্থাৎ বাক্যটার সত্যতা প্রমাণ করার কোনো কায়দা চোখে পড়ছে না। কিন্তু বাক্যটাকে ভুল কি প্রমাণ করতে পারবে, মানে বাক্যটার negation-কে ঠিক দেখাতে পারবে? Negation-টা হল

$$\exists x\in\phi\quad x\notin\{1,2\}.$$

অর্থাৎ এমন x নাকি আছে ϕ-এর মধ্যে যেটা $\{1,2\}$-তে নেই! সেটা তো স্পষ্টতঃই ভুল, কারণ ϕ-এর মধ্যে কোনো x-ই নেই! সুতরাং negation-টা ভুল, অতএব মূল বাক্যটা ঠিক ছিল। এইক্ষেত্রে আমরা বলব যে মূল বাক্যটা vacuously true.

DAY 2
দুটো set-কে সমান দেখানো

আমরা গতকাল শিখেছি কীভাবে কোনো কিছু প্রমাণ করতে হয়। বিশেষ করে শিখেছি দুটো set A আর B দেওয়া থাকলে কী করে $A=B$ দেখাতে হয়। প্রমাণটা দুইভাগে করতে হয়--প্রথমে দেখাতে হয় $A\subseteq B$, মানে A-র যে কোনো সদস্যই B-এরও সদস্য, অর্থাৎ অংকের ভাষায়

$$\forall a\in A\quad a\in B,$$

এবং তার পরে দেখাতে হয় $B\subseteq A$, মানে

$$\forall b\in B\quad b\in A.$$

আজকে আর আগামী কাল আমরা অনেকগুলো অংক করব যাদের সবারই মূল ব্যাপার হল দুটো set-কে সমান দেখানো, এবং বারবার আমরা এই একই কায়দা প্রয়োগ করব।

Example 7: Let A,B and C denote the subsets of a set S and C' denote the complement of C in S. If $A\cap C=B\cap C$ and $A\cap C'=B\cap C'$ then prove that $A=B$.[2] **(1997,2012.14i)**

SOLUTION:

এই অংকটার বক্তব্যটাকে একটু গল্প দিয়ে বুঝে নিই--নিবারণস্যারের কোচিংএর ছাত্রছাত্রীরা বরাবরই ভালো রেজাল্ট করে, কিন্তু এবারের রেজাল্ট একটু বেশীই ভালো। পাড়ার যত ছেলে নিবারণস্যারের কোচিংএ পড়ে তারা সবাই ফার্স্ট ক্লাস পেয়েছে, এবং তার বাইরে পাড়ার আরো কোনো ছেলে ফার্স্ট ক্লাস পায় নি! মজার কথা হল মেয়েদের ক্ষেত্রেও ঠিক একই ব্যাপার, পাড়ার যে কটা মেয়ে নিবারণস্যারের কোচিংএ পড়ত, তারা সবাই ফার্স্ট ক্লাস পেয়েছে, এবং তার বাইরে পাড়ার একটা মেয়েও ফার্স্ট ক্লাস পায় নি। সুতরাং এক কথায় নিবারণস্যারের জয়জয়কার--ওনার কোচিংএ পড়া আর ফার্স্ট ক্লাস পাওয়া সমার্থক! তুমি কি বুঝতে পারলে যে এই গল্পটা আসলে আমাদের অংকটাই? কিভাবে দ্যাখো--ধরো S হল পাড়ার সব ছাত্রছাত্রী, আর A হল এর মধ্যে নিবারণস্যারের কোচিংএর ছাত্রছাত্রীদের set, আর B হল যারা ফার্স্ট ক্লাস পেয়েছে তাদের set. বোঝার জন্য Fig 18



Fig 18

দ্যাখো। এবার C নেব ছেলেদের set. সুতরাং C' (মানে C-এর complement) হবে মেয়েদের set. সুতরাং নিবারণস্যারের কোচিংএর ছেলেরা হল $A \cap C$, আর ফার্স্ট ক্লাস পাওয়া ছেলেরা হল $B \cap C$. বলা হয়েছে যে এই দুটো set সমান (কারণ নিবারণস্যারের কোচিংএর ছাত্ররাই খালি ছেলেদের মধ্যে ফার্স্ট ক্লাস পেয়েছে)। সুতরাং $A \cap C = B \cap C$. একইভাবে মেয়েদের কথা ভাবলে পাবে $A \cap C' = B \cap C'$. এ থেকে নিবারণস্যারের জয়জয়কার--$A = B$, মানে নিবারণস্যারের কোচিংএ পড়া আর ফার্স্ট ক্লাস পাওয়া সমার্থক। এবার এটাই আমরা অংকের ভাষায় প্রমাণ করব।

> To Show: $A = B$,

দুটো set-কে সমান দেখাতে হবে, তার মানে--

> Step 1: Shall show $A \subseteq B$, ie
>
> $\forall x \in A \quad x \in B$.
>
> Take any $x \in A$.

এবার দুটো কেসে ভেঙে নেব--

> Then either $x \in C$ or $x \in C'$.

প্রথম কেসে ব্যবহার করব $A \cap C = B \cap C$.

> Case I: If $x \in C$, then
>
> $$x \in A \cap C = B \cap C \subseteq B.$$
>
> So $x \in B$.

দ্বিতীয় কেসে ব্যবহার করব $A \cap C' = B \cap C'$.

> Case 2: If $x \in C'$, then
>
> $$x \in A \cap C' = B \cap C' \subseteq B.$$
>
> So $x \in B$.
>
> Thus in both cases $x \in B$, as required.

> Since $x \in A$ was arbitrary, this proves $A \subseteq B$.

এবার বাকী অর্ধেক দ্যাখানোর পালা।

> Step 2: Shall show $B \subseteq A$.

কিন্তু যেহেতু ধাপগুলো একেবারেই একই থাকবে, খালি A-র জায়গায় B, আর B-এর জায়গায় A বসবে, তাই সহজে লিখে দিতে পারি--

> Interchanging A and B, we similarly have that $B \subseteq A$, completing the proof that $A = B$, as required.

■

Example 8: If A, B, C are three nonempty sets, prove that

$$A \cap (B - C) = (A \cap B) - (A \cap C).$$

[3] **(2002)**

SOLUTION: এই অংকটা নিয়ে একটা গল্প বানাই। সঙ্গীতা তার বান্ধবীদের চুপিচুপি বলেছে কী রকম মানুষ সে বিয়ে করতে চায়--ছেলেটা যেন পড়াশোনায় ভালো হয়, কিন্তু বেশী মোটা মায়নার চাকরী না করে। অতএব সঙ্গীতার মনের মানুষ যোগান দেবার দায়িত্ব যদি আমাদের উপর পড়ে তবে আমরা প্রথমেই একটা ফর্দ করে ফেলব সেই সব ছেলেদের যারা পড়াশোনায় ভালো, তারপর সেই ফর্দ থেকে মোটা মায়নার চাকরী করা ছেলেদের নাম কেটে দেব। লক্ষ কর যে, A যদি হয় ছেলেদের set আর B এবং C হয় যথাক্রমে "পড়াশোনায় ভালো"-দের set, আর "মোটা মায়নার চাকরী করা"-দের set, তবে সঙ্গীতার মনের মানুষকে খুঁজতে হবে এই set-এ--

$$A \cap (B - C).$$

আমরা যে সব পড়াশোনায় ভালো ছেলেদের তালিকা বানিয়েছিলাম, সেটা আসলে $A \cap B$. এ থেকে বাদ দিয়েছিলাম $A \cap C$, মানে মোটা মাইনের ছেলেদের set-টা। সুতরাং দাঁড়ালো

$$A \cap (B - C) = (A \cap B) - (A \cap C),$$

ঠিক যেটা আমাদের প্রমাণ করতে দিয়েছে। সঙ্গীতার বিয়ের নেমন্তন্নে যাওয়ার আগে নীচের প্রমাণটা শিখে নিতে ভুলো না! প্রথমে লিখে নিই কী দেখাতে যাচ্ছি--

> To show:
> $$A \cap (B - C) = (A \cap B) - (A \cap C),$$
>
> Step 1: Shall show
>
> $A \cap (B - C) \subseteq (A \cap B) - (A \cap C)$, ie,
>
> $\forall x \in A \cap (B - C) \quad x \in (A \cap B) - (A \cap C)$.

এখানে একটা $x \in A \cap (B - C)$ নিয়ে শুরু করে দেখাব যে সেই x-টা $(A \cap B) - (A \cap C)$-এর মধ্যেও আছে।

$\boxed{\forall x}$ Take any $x \in A \cap (B - C)$.

Then $x \in A$ and $x \in B - C$

মনে রেখো যে $x \in (B - C)$ মানে x আছে B-র মধ্যে, কিন্তু C-এর মধ্যে নেই।

$\therefore x \in A$ and $x \in B$ and $x \notin C$

যেহেতু x একইসঙ্গে A এবং B দুটোতেই আছে, তার মানে $A \cap B$-তে আছে। আবার x যেহেতু C-তে নেই, সুতরাং $A \cap C$-তেও থাকতে পারে না।

$\therefore x \in A \cap B$ and $x \notin A \cap C$,
$\therefore x \in (A \cap B) - (A \cap C)$, as required.

এবার উল্টো দিকটা দেখানোর পালা।

Step 2: Shall show
$(A \cap B) - (A \cap C) \subseteq A \cap (B - C)$, ie,
$\forall x \in (A \cap B) - (A \cap C) \quad x \in A \cap (B - C)$.

$\boxed{\forall x}$ Take any $x \in (A \cap B) - (A \cap C)$.

Then $x \in A \cap B$ and $x \notin A \cap C$.
$\implies x \in A$ and $x \in B$ and $x \notin A \cap C$.

এখানে $x \notin A \cap C$ মানে হয় $x \notin A$ আর নয়তো $x \notin C$. কিন্তু বলেই দিয়েছে যে $x \in A$. সুতরাং $x \notin A \cap C$ হওয়ার একটাই পথ--$x \notin C$.

$\implies x \in A$ and $x \in B$ and $x \notin C$.
$\implies x \in A \cap (B - C)$.

■

নীচে একই রকম আরেকটা অংক রয়েছে। এবার আর কোনো গল্প বানিয়ে দেব না। অংকটা পড়ে তুমি একটা গল্প বানাতে পারো?

Example 9: If A, B, C are three nonempty sets such that

$$A \cap B = A \cap C \text{ and } A \cup B = A \cup C,$$

then prove that $B = C$.[3] **(2001,2005)**
SOLUTION: মনে রেখো যে, দুটো set-কে সমান দেখানো মানে এটা দেখানো যে, ওরা পরস্পরের subset.

To show: $B = C$, ie, $B \subseteq C$, and $C \subseteq B$.

এবার এই দুটোকে দুই ধাপে প্রমাণ করব--

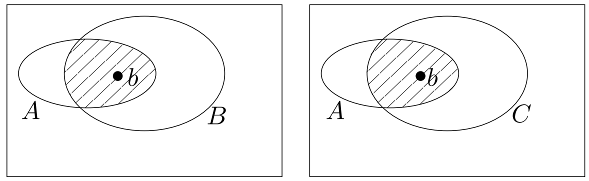


Fig 19

Step 1: Shall show: $B \subseteq C$, ie,

$\forall b \in B \quad b \in C.$

তার মানে B-র যে কোনো একটা element নিয়ে দেখাব যে সেটা C-এর মধ্যেও আছে।

$\forall b$ Take any $b \in B$.

এখন এই b-টা A-র ভিতরেও পড়তে পারে, বাইরেও পড়তে পারে। এই দুটো কেসকে আলাদা করে দেখব।

Then either $b \in A$ or $b \notin A$.

Case 1: $b \in A$:

এই কেসের ছবিটা দ্যাখো (Fig 19)। এখানে b রয়েছে $A \cap B$-তে। কিন্তু $A \cap B = A \cap C$, তাই b অবশ্যই $A \cap C$-তেও আছে।

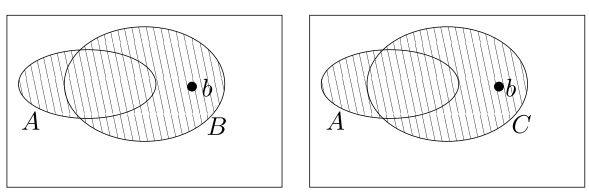
Here $b \in A \cap B = A \cap C \subseteq C$.
So $b \in C$.

এবার দেখি b-টা A-র বাইরে থাকলে কি হয়। Fig 20 দ্যাখো।

Case 2: $b \notin A$:
Since $b \in B$ so $b \in A \cup B = A \cup C$.
Also $b \notin A$.
So $b \in C$.

সুতরাং দুটো কেস মিলিয়ে পাই--

Fig 20



> Hence in both cases $b \in C$, as required.

এবার তবে দেখানো উচিত যে $C \subseteq B$. কিন্তু লক্ষ কর যে, আমরা যা যা করেছি, তার মধ্যে B-এর জায়গায় C, আর C-এর জায়গায় B লিখলে তার কিছুই বদলাত না। তাই এখানে এককথায় লিখে দিতে পারি যে--

> Step 2: Similarly, interchanging B, C above, we have $C \subseteq B$.
> Hence $B = C$, as required.

■

Example 10: Give suitable examples to show that only $A \cup B = A \cup C$ or only $A \cap B = A \cap C$ does not necessarily imply $B = C$.[2] **(2009.2aii)**

SOLUTION: এটা এক অর্থে আগের অংকটার উল্টো। আগের অংকটায় আমরা দেখিয়েছিলাম যে, একইসঙ্গে $A \cup B = A \cup C$ এবং $A \cap B = A \cap C$ হলে $B = C$ হতে বাধ্য। এই অংকে প্রশ্ন হল যদি খালি $A \cup B = A \cup C$ হয় বা খালি $A \cap B = A \cap C$ হয়, তবেও কি $B = C$ হবেই? উত্তরটা অবশ্য বলেই দিয়েছে--না। আমাদের কাজ হল counterexample দিয়ে এটা দেখানো। বস্তুতঃ এখানে দুটো counterexample লাগবে--

- প্রথম counterexample-এর জন্য এমন তিনটে A, B, C খুঁজব যাতে $A \cup B = A \cup C$ হয় কিন্তু $B \neq C$ হয়।
- দ্বিতীয়টার জন্য চাই এমন A, B, C যাতে $A \cup B = A \cup C$ হয় কিন্তু $B \neq C$ হয়।

প্রথম counterexample-টা হতে পারে এরকম--প্রথমে B আর C যা খুশি আলাদা আলাদা দুটো set নাও, তারপর A এমন কিছু নাও যার মধ্যে B, C দুজনেই আছে, তাহলে $A \cup B$ আর $A \cup C$ নিলে B এবং C-এর পার্থক্যটা চাপা পড়ে যাবে।

> Let $A = \{1, 2\}$, $B = \{1\}$ and $C = \{2\}$.
> Then $A \cup B = A \cup C = S$, but $B \neq C$.

দ্বিতীয় counterexample-টাও একইরকম--

> Let $A = \phi, B = \{1\}, C = \{2\}$.
> Then $A \cap B = A \cap C = \phi$, but $B \neq C$.

■

Example 11: If A is a fixed nonempty subset of a set S such that for all nonempty subsets B of S,

$$A \cup B = B,$$

then prove that $A = \phi$.[2] **(2005)**

SOLUTION: এই অংকটা অতি হাস্যকর রকমের ভুল। শুরুতেই বলে দিয়েছে যে A হল nonempty, অথচ শেষে প্রমাণ করতে বলেছে $A = \phi$! অবশ্য প্রথমে যদি A-কে nonempty নাও বলে দিত, তাও অংকটা ভুল। তার জন্য একটা counterexample এইরকম-- ধরো আমরা $S = \{1\}$ আর $A = \{1\}$ নিলাম। তাহলে S-এর যে কোনো nonempty

subset B-এর জন্যই $A \cup B = B$ হবে, কারণ S-এর nonempty subset বলতে আছে তো খালি একটাই--$B = \{1\}$. সুতরাং

$$A \cup B = \{1\} \cup \{1\} = \{1\} = B.$$

কিন্তু দেখতেই পাচ্ছ যে $A \neq \phi$. ■

এই ভুল অংকটাকে অন্ততঃ দুইভাবে মেরামত করা যায়। এ থেকেই নীচের দুটো অংকের জন্ম--

Exercise 7: If A is a fixed subset of a set S such that for all subsets B of S,

$$A \cup B = B,$$

then prove that $A = \phi$. ■

Exercise 8: If A is a fixed subset of a set S such that $A \neq S$ and for all nonempty subsets B of S,

$$A \cup B = B,$$

then prove that $A = \phi$. ■

Example 12: Prove that $(A \cap C) \cup (B \cap C') = \phi \implies A \cap B = \phi$.[2] **(2011.14i)**

SOLUTION: এই অংকটা নিয়ে চিন্তা করা যায় এইভাবে। $(A \cap C) \cup (B \cap C') = \phi$ বলে দিয়েছে, তার মানে $(A \cap C)$ এবং $(B \cap C')$ দুজনেই ϕ. এখন $A \cap C = \phi$ মানে হল A-র কোনো অংশই C-এর মধ্যে নেই, অর্থাৎ A পুরোটাই আছে C-এর বাইরে। একইভাবে $B \cap C' = \phi$ মানে B পুরোটাই আছে C-এর মধ্যে। যেহেতু A আছে C-এর বাইরে, আর B আছে C-এর ভিতরে, তাই বোঝাই যাচ্ছে যে, $A \cap B = \phi$ হবেই।
লেখার সময়ে আমরা proof by contradiction লাগাব--

> Let, if possible, $A \cap B \neq \phi$.
> We pick $x \in A \cap B$.
> Either $x \in C$ or $x \in C'$.
> Case 1: If $x \in C$, then
>
> $$x \in A \cap C \subseteq (A \cap C) \cup (B \cap C') = \phi (\Rightarrow\Leftarrow).$$
>
> Case 2: If $x \in C'$, then
>
> $$x \in B \cap C' \subseteq (A \cap C) \cup (B \cap C') = \phi (\Rightarrow\Leftarrow).$$
>
> So $A \cap B = \phi$, as required.

■

Exercise 9: Show that for any three non-empty sets X, Y, Z,

$$(X \cap Z) \cup (Y \cap Z') = \phi \implies X \cap Y = \phi.$$

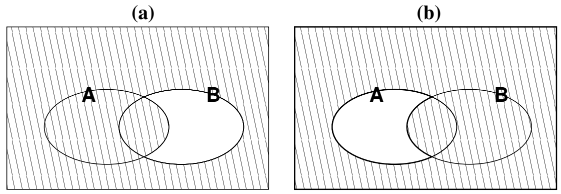


Fig 21

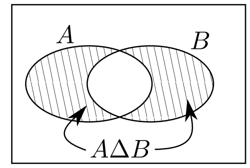


Fig 22

[2]
HINT:
আগের অংকটাই। এখানে non-empty শর্তটার কোনো দরকার নেই।
■

Example 13: State true or false with justification: $(A - B)' = (B - A)'$ where the symbol C' denotes the complement of C. **(2008)**
SOLUTION: True হবে না false হবে সেটা একটা Venn diagram আঁকলেই বোঝা যাবে (Fig 21)। দ্যাখাই যাচ্ছে যে shaded অংশদুটো দুটো ছবিতে এক নয়। সুতরাং--

> The result is false.

কিন্তু একটা ছবি এঁকে একথাটা বলে দিলেই চলবে না, দস্তুরমত একটা counterexample চাই। সেটা অবশ্য ছবি থেকেই বার করব। Fig 21(a) আর (b)-র shaded region দুটোর দিকে তাকালেই দেখবে ওদের মূল পার্থক্য ওই চাঁদের মত অংশ দুটোতে। অতএব যদি A, B এমনভাবে নিই যাতে দুটো চাঁদের অন্ততঃ একটাও nonempty হয়, তবেই counterexample পাব। Set-এর ভাষায় চাঁদদুটো হল $A \setminus B$ আর $B \setminus A$. আমরা নীচের উদাহরণে $A - B$-টাকে nonempty নিয়েছি।

> If the universal set is $\{1, 2\}$, $A = \{1, 2\}$ and $B = \{2\}$, then $(A \setminus B)' = \{1\}' = \{2\}$.
> But $(B \setminus A)' = \phi' = \{1, 2\} \neq (A \setminus B)'$.

লক্ষ কর যেহেতু আমরা complement নিয়ে কাজ করছি, তাই আলাদা করে universal set-টার উল্লেখ করতে হয়েছে। ■

Example 14: Either prove or disprove with the help of a counterexample

$$(A \setminus B)' = (B \setminus A)'.$$

[2] **(2010.2aii)**
SOLUTION: আগের অংকটাই। ■

যদি চাঁদের মত অংশদুটোর union নিই, তবে যে set-টা পাব তাকে বলে **symmetric difference.** এটা আমরা আগেই শিখেছিলাম। দুটো set-এর নাম যদি A, B হয় তবে ওদের symmetric difference-কে লেখে $A\Delta B$. Fig 22 দ্যাখো।

Example 15: Prove that an equivalent definition of symmetric difference of two sets A and B is

$$A\Delta B = (A\cup B)\setminus(A\cap B).$$

[3] **(2010.2ai)**

SOLUTION: এই অংকটার বক্তব্য হল দুটো চাঁদের union-কে আমরা "বাইনোকুলার থেকে চোখ বাদ" বলেও ভাবতে পারি।

By definition

$$A\Delta B = (A\setminus B)\cup(B\setminus A).$$

Shall show $A\Delta B = (A\cup B)\setminus(A\cap B)$.

Step 1: Shall show $A\Delta B \subseteq (A\cup B)\setminus(A\cap B)$, ie,

$\forall x\in A\Delta B \quad x\in(A\cup B)\setminus(A\cap B)$.

$\forall x$ Take any $x\in A\Delta B$.

Then either $x\in A\setminus B$ or $x\in B\setminus A$.

Case 1: If $x\in A\setminus B$, then $x\in A$ and $x\notin B$.

$\therefore x\in A\cup B$ and $x\notin A\cap B$.

So $x\in(A\cup B)\setminus(A\cap B)$, as required.

Case 2: If $x\in B\setminus A$, then $x\in B$ and $x\notin A$.

$\therefore x\in A\cup B$ and $x\notin A\cap B$.

So $x\in(A\cup B)\setminus(A\cap B)$, as required.

Step 2: Shall show $(A\cup B)\setminus(A\cap B)\subseteq A\Delta B$, ie,

$\forall y\in(A\cup B)\setminus(A\cap B) \quad y\in A\Delta B$.

$\forall y$ Take any $y\in(A\cup B)\setminus(A\cap B)$.

Then $y\in A\cup B$ but $y\notin A\cap B$.

Case 1: If $y\in A$, then $y\notin B$, since otherwise $y\in A\cap B$.

So $y\in A\setminus B\subseteq A\Delta B$.

Case 2: If $y\notin A$, then $y\in B$, since otherwise $y\notin A\cup B$.

So $y\in B\setminus A\subseteq A\Delta B$.

Thus, in either case, $y\in A\Delta B$, as required.

■

DAY 3
আরও প্রয়োগ

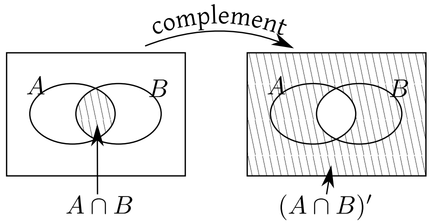


Fig 23

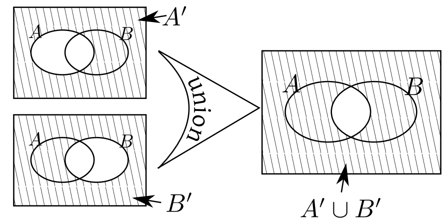


Fig 24

3.1 de Morgan's Laws

ভারতের উত্তর-পশ্চিমে পাকিস্তান-সীমান্ত ঘেঁসে সিয়াচেন হিমবাহের নাম তোমরা হয়তো শুনেছ। সেখানে একবার আমাদের পাড়ার ট্রেকিং ক্লাব থেকে অভিযানে যাবার কথা উঠেছিল। সীমান্ত অঞ্চল তো, যাবার জন্য দস্তুরমত মিলিটারী অনুমতি লাগে। অনুমতি পেতে গেলে দুটো শর্ত--

1. ভারতীয় নাগরিক হতে হবে ,এবং
2. পাহাড়ে চড়ার সরকারী ট্রেনিং থাকতে হবে।

সুতরাং অনুমতি পাবে না কারা? যারা ভারতীয় নয় অথবা যাদের ট্রেনিং নেই। যাদের ট্রেনিং আছে তাদের set-কে যদি A বলি, আর ভারতীয় নাগরিকদের set-কে যদি B বলি, তবে অনুমতি পেতে হলে তোমাকে এই দুটো set-এর মধ্যেই পড়তে হবে, মানে $A \cap B$-এর element হতে হবে। সুতরাং অনুমতি যারা পাবে না, মানে $(A \cap B)'$, তারা হয় A'-এ আছে বা B'-এ আছে। সুতরাং পেলাম--

$$(A \cap B)' = A' \cup B'$$

একে বলে de Morgan-এর একটা সূত্র[1]। de Morgan-এর অন্য সূত্রটা হল--

$$(A \cup B)' = A' \cap B'.$$

এই দুটোকে একসাথে বলে de Morgan's laws. ছবি দিয়ে বোঝানো আছে Fig 23 আর Fig 24-তে।

এইবার আমরা কিছু অংক করব যেখানে দুটো set-কে সমান দেখাতে হবে। এখানে de Morgan-এর law-দুটো লাগালে কাজ অনেক সহজ হয়ে যাবে। মনে রেখো যে, দুইধাপে ভেঙে যেভাবে অংক করছিলাম (মানে $A = B$ দেখানোর জন্য আলাদা করে $A \subseteq B$ আর $B \subseteq A$ দেখানো) সেই পদ্ধতি কিন্তু এদের ক্ষেত্রেও প্রযোজ্য। কিন্তু de Morgan লাগালে এখানে কম লিখতে হবে।

কী করে বুঝব কোথায় de Morgan লাগালে ভালো? তার জন্য de Morgan-এর মার্কামারা চেহারাটা চিনে রাখো-- যদি $A' \cup B'$ বা $A' \cap B'$ দ্যাখো (অর্থাৎ $\cap$ বা $\cup$-এর দুধারেই দুটো complement, অমনি বুঝবে যে de Morgan লাগানোর সময় উপস্থিত। একইভাবে যদি কখনো $(A \cap B)'$ বা $(A \cup B)'$ পাও, তবেও জানবে de Morgan লাগানো যেতে পারে। যেমন $(a+b)^2$ দেখলেই হাত নিশপিশ করে ওঠে $a^2 + b^2 + 2ab$ লেখার জন্য তেমনি $(A \cup B)'$ দেখলেই হাত নিশপিশ করে ওঠা উচিত ব্র্যাকেট তুলে ওটাকে $A' \cap B'$ লেখার জন্য, কিংবা $(A \cap B)'$-কে $A' \cup B'$ লেখার জন্য।

যে কটা আমরা অংক আমরা করতে চলেছি, তার মধ্যে প্রথম অংকটাতে অবশ্য de Morgan লাগালে চলবে না, কারণ de Morgan-এর একটা সূত্র দুটোর একটাকেই এখানে প্রমাণ করতে দেওয়া হয়েছে।

Example 16: Let A, B be two subsets of a set S. Prove that $(A \cap B)' = A' \cup B'$ where C' denotes the complement of a subset C in S.[3] **(1998)**

SOLUTION: যেকোনো দুটো set-কে সমান দেখানোর মূল পদ্ধতি একটাই--এটা দেখানো যে প্রথম set-টা দ্বিতীয় set-এর subset, আবার দ্বিতীয় set-টা প্রথম set-টার subset.

[1] এবং এটা সিয়াচেনের বাইরেও খাটে!

To show $(A \cap B)' = A' \cup B'$.
Step 1: Shall show $(A \cap B)' \subseteq A' \cup B'$,
ie,
$\forall x \in (A \cap B)' \quad x \in A' \cup B'$.
$\boxed{\forall x}$ Take any $x \in (A \cap B)'$.

এর পর বস্তুতঃ খালি সংজ্ঞার প্রয়োগ করে গেলেই হবে। কোনো set-এর complement-এ থাকা মানে, সেই set-এ না থাকা, সুতরাং--

So $x \notin A \cap B$,

এর মানে x-টা একই সঙ্গে A এবং B-তে নেই। তার মানে হয় x-টা A-তে নেই, নয় B-তে নেই।

So either $x \notin A$ or $x \notin B$,

আবার complement-এর সংজ্ঞা লাগাই--

ie, either $x \in A'$ or $x \in B'$,

তারপর $\cup$-এর সংজ্ঞা--

ie, $x \in A' \cup B'$, completing step 1.

এইবার উল্টো দিকটা--

Step 2: Shall show $A' \cup B' \subseteq (A \cap B)'$,
ie,
$\forall x \in A' \cup B' \quad x \in (A \cap B)'$.
$\boxed{\forall x}$ Take $x \in A' \cup B'$.
Then either $x \notin A$ or $x \notin B$.
If $x \notin A$ then $x \notin (A \cap B)$, ie, $x \in (A \cap B)'$.
Similarly, if $x \notin B$ then $x \notin (A \cap B)$, ie, $x \in (A \cap B)'$.
So in both cases $x \in (A \cap B)'$, completing step 2.

বিকল্প পদ্ধতি

একটু ভালো করে দেখলেই বুঝবে যে দুটো ধাপ সম্পূর্ণভাবে একে অপরের বিপরীত। এরকম ক্ষেত্রে আমরা ইচ্ছে করলে দুটো ধাপকে একসাথে জুড়ে লিখতে পারি এইভাবে--

Let the universal set be S.
To show: $(A \cap B)' = A' \cup B'$,
ie, $\forall x \in S \quad x \in (A \cap B)' \iff x \in A' \cup B'$.
Take any $x \in S$.
Then

$$\begin{aligned} x \in (A \cap B)' &\iff x \notin (A \cap B) \\ &\iff x \notin A \text{ or } x \notin B \\ &\iff x \in A' \text{ or } x \in B' \\ &\iff x \in A' \cup B'. \end{aligned}$$

So $(A \cap B)' = A' \cup B'$, as required.

মনে রেখো যে একসাথে দুটো ধাপ জুড়ে দেওয়া কিন্তু সবসময়ে যায় না। কেবল খুব সহজ অংকের ক্ষেত্রেই করা যায়। দুটো ধাপ আলাদা করে করার পদ্ধতিটা কিন্তু সবসময়েই কাজ করে। ■

Exercise 10: একইভাবে প্রমাণ করার চেষ্টা কর যে $(A \cup B)' = A' \cap B'$. ■

এবার আমরা de Morgan-এর কিছু প্রয়োগ দেখব।

Example 17: B and C are nonempty subsets of a set A. Show that

$$[A \cup (B' \cap C')]' = \phi(\text{null set}),$$

where A' denotes the complement of A.[2] **(2004)**
SOLUTION: একবার বাঁদিকটার দিকে তাকিয়ে দেখলেই বুঝবে যে de Morgan লাগানোর অপেক্ষায় তৈরী। বস্তুতঃ দুবার de Morgan লাগানো যাবে--

By de Morgan,

$$[A \cup (B' \cap C')]' = A' \cap (B' \cap C')' = A' \cap (B \cup C),$$

since $(B')' = B$ and $(C')' = C$.

এইবার ব্যবহার করব যে $B, C \subseteq A$.

But since $B, C \subseteq A$ so $B \cup C \subseteq A$. So

$$A' \cap (B \cup C) \subseteq A' \cap A = \phi.$$

Since ϕ has only one subset ϕ,

$$\therefore A' \cap (B \cup C) = \phi.$$

ব্যস্, অংক শেষ। লক্ষ কর, প্রশ্নে যে B, C-কে nonempty দেওয়া ছিল, তার আসলে কোনো দরকারই হল না।

Hence $[A \cup (B' \cap C')]' = \phi$, as required.

■

Example 18: A, B, C are subsets of a universal set S. Prove that

$$[A \cap (B \cup C)] \cap [A' \cup (B' \cap C')] = \phi,$$

where D' denotes the complement of a subset D in S.[2] **(2006)**
SOLUTION:

By de Morgan's law

$$A' \cup (B' \cap C') = A' \cup (B \cup C)' = [A \cap (B \cup C)]'.$$

Since for any set D we have $D \cap D' = \phi$, so taking $D = [A \cap (B \cup C)]$ the result follows.

■

Example 19: State true or false with justification: A, B, C are three nonempty sets and $A \subseteq B \subseteq C$ then $A' \subseteq B' \cup C'$. (For any set A, A' is its complement.) **(2003)**
SOLUTION: ডানদিকে আছে $B' \cup C'$, যেটা দেখলেই de Morgan-এর কথা মনে পড়ে। যদি de Morgan লাগাই তবে পাব

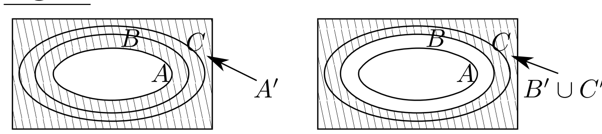
$$A' \subseteq (B \cap C)'.$$

যদি দুইদিকেই complement নিই তবে $\subseteq$-টা উল্টে গিয়ে হবে

$$A \supseteq (B \cap C).$$

এটা অপেক্ষাকৃত ভদ্রসভ্য দেখতে, কোনো complement-টম্‌প্লিমেন্টের বালাই নেই। এটাকে আরো সহজে লেখা যায়। যেহেতু $B \subseteq C$ সুতরাং $B \cap C = B$. তার মানে আমাদের পরীক্ষা করে দেখতে হবে $A \supseteq B$ হচ্ছে কিনা। প্রশ্নে A আর B-কে নিয়ে খালি বলা আছে $A \subseteq B$. তা থেকে খামোখা $A \supseteq B$ হতে যাবে কেন? সুতরাং উত্তর নিশ্চয়ই false হবে। ভালো করে নিশ্চিত হতে একটা ছবি এঁকে নেওয়া যাক Fig 25 দ্যাখো। এখানে দেখাই যাচ্ছে যে, A' হল $B' \cup C'$-এর চেয়ে কিছুটা বড়।

Fig 25



> The result is false.

যদি কোনোকিছু ভুল দেখাতে চাই তবে সবচেয়ে ভালো পথ হচ্ছে একটা counterexample দেখানো। তার জন্য এমন A, B নেব যাতে $A \subseteq B$ হয়, কিন্তু $A \supseteq B$ না হয়ে যায়, মানে $A \subsetneq B$ হয়।

> Take the universal set $\{1, 2, 3, 4\}$ and
> $$A = \{1\}, \quad B = \{1, 2\}, \quad C = \{1, 2, 3\}.$$

এখানে গুরুত্বপূর্ণ ব্যাপার একটাই, সেটা হল B-এর মধ্যে ওই 2 element-টা। এই 2-টা A-র মধ্যে নেই, তাই, $A \subsetneq B$ হচ্ছে।

> Then $A \subseteq B \subseteq C$. But $A' = \{2, 3, 4\}$ and $B' \cup C' = \{3, 4\}$. So $A \not\subseteq B' \cup C'$.

■

3.2 Cartesian products

দুটো set দেওয়া থাকলে তাদের মিলিয়ে একটা নতুন set বানাবার অনেক কায়দা আছে, যেমন union, intersection ইত্যাদি। এবার যে অংকগুলো করব সেখানে দুটো set মিলিয়ে অন্য একটা পথে নতুন set বানাব, **Cartesian product** দিয়ে। ব্যাপারটা এইরকম। ধর একজন সিনেমার ডিরেকটর একটা নতুন ছবির জন্য নায়ক নায়িকা খুঁজছেন। তাঁর কাছে নায়ক আছেন দুজন $A = \{$জিৎ, দেব$\}$ আর নায়িকা তিনজন $B = \{$ঋতুপর্ণা, রাইমা, কোয়েল$\}$. তাহলে ভদ্রলোক কী কী ভাবে নায়ক-নায়িকা নিতে পারবেন? উত্তর হল, এই কয়ভাবে--

$C = \big\{$(জিৎ, ঋতুপর্ণা), (জিৎ, রাইমা), (জিৎ, কোয়েল),
(দেব, ঋতুপর্ণা), (দেব, রাইমা), (দেব, কোয়েল)$\big\}$.

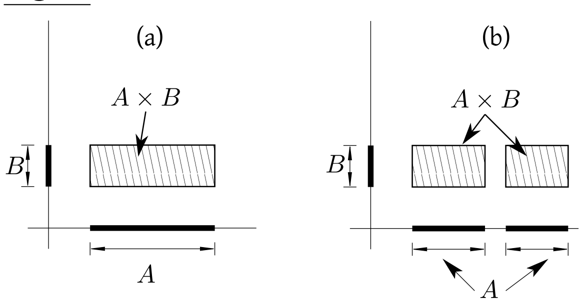
এখানে প্রত্যেকটা জুটিকে অংকের ভাষায় বলে একেকটা ordered pair. কেন pair বলে সেটা তো বুঝতেই পারছ, আর ordered বলার কারণ এই যে, প্রত্যেক ক্ষেত্রেই আমরা প্রথমে নায়ক, পরে নায়িকা এই order-টা (মানে কে আগে কে পরে, সেটা) রক্ষা করেছি, যেমন (দেব, কোয়েল)-কে আমরা কখনো (কোয়েল, দেব) লিখিনি। এই যে ছয়টা সম্ভাব্য জুটির set-টা পেলাম তাকে বলে নায়কের set আর নায়িকার set-এর Cartesian product এবং লেখে

$$C = A \times B.$$

তার মানে প্রথম set-টা থেকে একটা করে আর দ্বিতীয় set-টা থেকে একটা করে element নিয়ে পাওয়া যাবতীয় ordered pair-এর set-টাকেই বলে set দুটোর Cartesian product.

এদের সম্বন্ধে নীচের কয়টা কথা মনে রাখা দরকার। ধরো A আর B যেকোনো দুটো set.

Fig 26



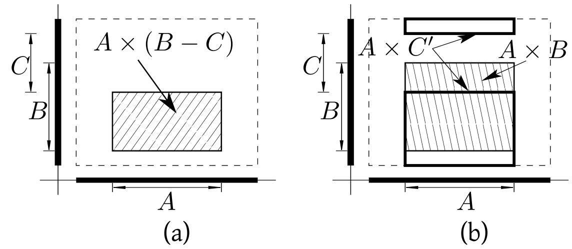


Fig 27

1. যদি বলি "$(x, y) \in A \times B$" তার মানে "$x \in A$ এবং $y \in B$." যদি বলতাম "$(x, y) \in B \times A$" তবে মানে হত "$x \in B$ আর $y \in A$." একইভাবে "$(x, y) \in A \times A$" মানে x, y দুজনেই A-র মধ্যে আছে-- $x, y \in A$.

2. গ্রাফ আঁকার সময়ে আমরা কোনো বিন্দুর অবস্থান বোঝাতে যে (x, y) ব্যবহার করি সেটা একটা ordered pair-এর উদাহরণ। এটা ordered কারণ (2,3) আর (3,2) আলাদা বিন্দু বোঝায়।

3. Set-এর অংকে সাধারণতঃ Venn diagram এঁকে নিলে সুবিধা হয়। Cartesian product-এর বেলায় ছবিটা একটু কায়দা করে গ্রাফের মত করে আঁকতে হয়। ধরো $A \times B$ আঁকতে চাই। প্রথমে গ্রাফের মত দুটো axis আঁকো। তার পর x-axis বরাবর A আর y-axis বরাবর B দেখাও, যেমন Fig 26(a)-তে করা হয়েছে।

   তাহলে shaded rectangle-টা হল $A \times B$. কারণ এই rectangle-এর যেকোনো বিন্দু হচ্ছে (x, y) যেখানে $x \in A$ আর $y \in B$. আমরা ইচ্ছে করলে A-কে Fig 26(b)-এর মত একটা দুই-টুকরো set-ও নিতে পারতাম। এখানে A হচ্ছে মোটা লাইনদুটোর union. এক্ষেত্রে $A \times B$-টাও দুটো টুকরো দিয়ে তৈরী।

Example 20: Define Cartesian product of two nonempty sets.[2] **(2003)**

SOLUTION:

DEFINITION: **Cartesian product of sets**

If A, B are two (nonempty) sets then by their Cartesian product we mean the set

$$A \times B = \{(a, b) : a \in A, \quad b \in B\}.$$

এখানে A, B-র মধ্যে একজনও যদি ϕ হত তবেও কিন্তু $A \times B$ নিয়ে কাজ করা যায়, খালি সেক্ষেত্রে $A \times B = \phi$ হবে।
■

Example 21: Show that

$$A \times (B - C) = (A \times B) \cap (A \times C'),$$

C' is the complement of C in S, where S is the universal set.[2] **(2013,2003)**

SOLUTION:

To show $A \times (B - C) = (A \times B) \cap (A \times C')$.

Fig 27 দ্যাখো।

মনে আছে নিশ্চয়ই যে, দুটো set-এ সমান দেখানো মানে এটা দেখানো যে এই set-এর সব element ওই set-এ আছে, আবার ওই set-এর সব element আছে এই set-এ। প্রথমে এই কথাটাকে লিখে শুরু করব।

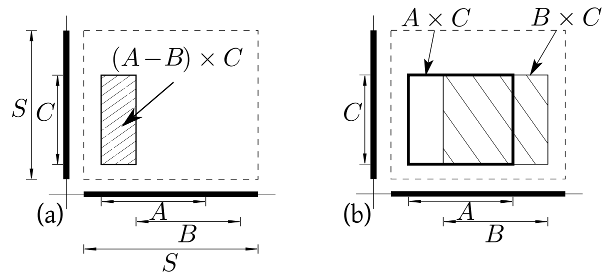


Fig 28

Take any $(x,y) \in S \times S$. We shall show that

$$(x,y) \in A \times (B-C) \iff (x,y) \in (A\times B) \cap (A \times C').$$

বাঁদিকে আছে $(x,y) \in A \times (B-C)$. Cartesian product-এর definition লাগিয়ে এটাকে ভেঙে ফেলব--

Now

$$\begin{aligned} & (x,y) \in A \times (B-C) \\ \iff & x \in A \quad \& \quad y \in (B-C) \\ \iff & x \in A \quad \& \quad y \in B \quad \& \quad y \notin C \\ \iff & (x,y) \in (A\times B) \quad \& \quad (x,y) \in (A \times C') \\ \iff & (x,y) \in (A\times B) \cap (A \times C'), \end{aligned}$$

as required.

■

Example 22: A, B, C are subsets of a universal set S. Prove that

$$(A-B)\times C = (A\times C) - (B\times C).$$

[3] **(2006)**
SOLUTION: এই অংকটাকেও আগের অংকটার মত করেই আক্রমণ করব। প্রথম কাজ ছবি এঁকে ফেলা (Fig 28)। তারপর লিখব যে ঠিক কী দেখাতে যাচ্ছি--

To show that

$$(x,y) \in (A-B)\times C \iff (x,y) \in (A\times C) - (B \times C).$$

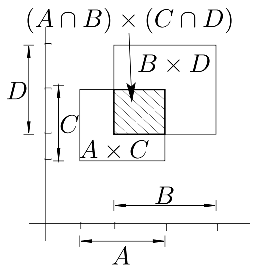


Fig 29

> Now
>
> $$\begin{aligned} & (x,y) \in (A - B) \times C \\ \iff & x \in (A - B) \quad \& \quad y \in C \\ \iff & x \in A \quad \& \quad x \notin B \quad \& \quad y \in C \\ \iff & (x,y) \in A \times C \quad \& \quad (x,y) \notin B \times C \\ \iff & (x,y) \in (A \times C) - (B \times C), \end{aligned}$$
>
> as required.

■

Example 23: Prove the following set theoretic statement if it is true or give counter example to disprove it:

$$A \times (B \setminus C) = (A \times B) \setminus (A \times C).$$

[3] **(2009.2ai)**
SOLUTION: একেবারেই আগের অংকটার মত, তাই আর করে দেব না। ■

Example 24: For any four nonempty sets A, B, C, D show that

$$(A \cap B) \times (C \cap D) = (A \times C) \cap (B \times D).$$

[3] **(2000,2004)**
SOLUTION: প্রথমে ছবি (Fig 29)।
তারপর কি দেখাব সেটা গুছিয়ে লেখা--

> To show that
>
> $$(x,y) \in (A \cap B) \times (C \cap D) \iff (x,y) \in (A \times C) \cap (B \times D).$$

Now

$$\begin{aligned} & (x,y) \in (A\cap B)\times(C\cap D) \\ \iff & x \in (A\cap B) \quad \& \quad y \in (C\cap D) \\ \iff & x\in A \quad \& \quad x\in B \quad \& \quad y\in C \quad \& \quad y \in D \\ \iff & (x,y)\in A\times C \quad \& \quad (x,y)\in B\times D \\ \iff & (x,y) \in (A\times C)\cap(B\times D), \end{aligned}$$

as required.

■

Exercise 11: নীচের কোন কোন বাক্যগুলো ঠিক বল তো।

1. $(x,x)\in A\times B \iff x\in A\cap B$.
2. $(x,x)\notin A\times B \iff x\in A^c\cap B^c$.
3. $(x,y)\in (A\times B)\cap(B\times A) \iff x,y\in A\cap B$.

■

DAY 4
Function (part 1)

Function ব্যাপারটার সঙ্গে হায়ার সেকণ্ডারী থেকেই আমাদের পরিচয় আছে, এবং function বলতেই আমাদের মনে $\sin x$ বা e^x বা x^2 জাতীয় জিনিস ভেসে ওঠে। অর্থাৎ হায়ার সেকণ্ডারীর অভিজ্ঞতা থেকে মনে হয় যে, একটা function $f(x)$ মানেই একটা ফর্মুলা। তার মধ্যে একটা variable থাকে (যেটাকে এখানে x দিয়ে লেখা হয়েছে)। যদি $x =$ কোনো সংখ্যা বসাই, তবে $f(x) =$ একটা সংখ্যা পাওয়া যায়। যেমন $f(x)=\sin x$-এ $x=\frac{\pi}{2}$ বসালে $f(x)=1$ পাব। অংকের জগতে কিন্তু function মাত্রেই সব সময়ে একটা ফর্মুলা নয়, আরো একটু general জিনিস, যেটা এবার আমরা শিখব। আমরা x-এর একটা value থেকে $f(x)$-এর একটা value পাই। তাই মনে করতে পারো যেন $f(x)$ একটা যন্ত্রের মত, যার মধ্যে x-এর value-টা input হিসেবে ঢুকিয়ে দিলে $f(x)$-এর value-টা output রূপে বেরিয়ে আসে (Fig 30)। এরকম যে

Fig 30

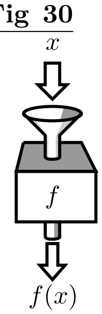


Fig 31



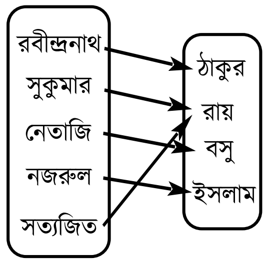


Fig 32

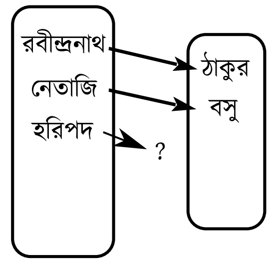


Fig 33

কোনো যন্ত্রকেই function বলা হয়, সেই যন্ত্রের পেটের ভিতর একটা ফর্মুলাও থাকতে পারে বা অন্য কিছুও থাকতে পারে, যেমন নীচের উদাহরণে।

Example 25: আমার মোবাইল ফোনে আমার বন্ধুদের নাম আর ফোন নম্বর ঢোকানো আছে। আমি যেই সুইচ টিপে টিপে একটা বন্ধুর নাম টাইপ করি, অমনি ফোনটা তার নম্বরটা দেখিয়ে দেয়। এটাও একটা function-এর উদাহরণ। এখানে input হল বন্ধুটার নাম, আর output হল তার ফোন নম্বর। এর মধ্যে কোনো ফর্মুলার গল্প নেই, আছে খালি একটা তালিকা (Fig 31) ■

যে কোনো function-এর সঙ্গেই তিনটে set জড়িত থাকে--

1. Domain: এটা হল যাবতীয় input-এর set, প্রতিটি সম্ভাব্য input হল domain-এর element.
2. Codomain: প্রতিটি সম্ভাব্য output-কে এই set-এর element হতে হবে।
3. Range: codomain-এর প্রতিটা element-ই যে একেকটা output হবে এমন কিন্তু কথা নেই। যারা output হতে পারে তাদের নিয়ে codomain-এর যে subset-টা হয়, তাকে বলে range.

যদি একটা function থাকে f যার domain হল A আর codomain হল B, তবে আমরা লিখি $f : A \to B$.

Example 26: ধরো $f(x) = x^2 - 2x$. এখানে x-এর জায়গায় কোনো real number বসালে $f(x)$ একটা real number হবে। তাই আমরা এখানে domain আর codomain দুটোই নিতে পারি $\mathbb{R}$. অর্থাৎ $f : \mathbb{R} \to \mathbb{R}$ লেখা যায়। কিন্তু $f(x)$ কি যে কোনো real number হতে পারে? লক্ষ কর যে, $f(x) = (x-1)^2 - 1$, তাই $f(x)$-এর পক্ষে -1-এর নীচে নামা সম্ভব নয়, কারণ $(x-1)^2 \geq 0$. কিন্তু $[1, \infty)$-র মধ্যে যে কোনো value-ই $f(x)$ নিতে পারে। তাই এখানে range হল $[1, \infty)$. ■

কোন্ input-এর ফলে কোন্ output বেরোবে সেই যোগাযোগটা ঠিক করে দেয় function-টা। এই যোগাযোগটা নানাভাবে প্রকাশ করা যায়--ফর্মুলা দিয়ে, বা গ্রাফ দিয়ে, বা তালিকা দিয়ে, বা তীর চিহ্ন দিয়ে। তীর চিহ্ন দিয়ে একটা function-কে এঁকে বোঝানো প্রথম প্রথম শেখার সময়ে খুব সুবিধাজনক, তাই একটা উদাহরণ দিয়ে বুঝে নিই।

Example 27: এই বিখ্যাত মানুষদের কথা তোমরা সবাই শুনেছ--

রবীন্দ্রনাথ, সুকুমার, নেতাজি, নজরুল, সত্যজিত।

যদি এদের কারোর নাম বলে তার পদবী জানতে চাই তবে, নিশ্চয়ই নামটুকু শুনেই তুমি তা বলে দিতে পারবে। তার কারণ তোমার মাথায় একটা function ঢোকানো আছে, যেটাকে তীর চিহ্ন দিয়ে আঁকলে Fig 32-এর মত হয়। ■

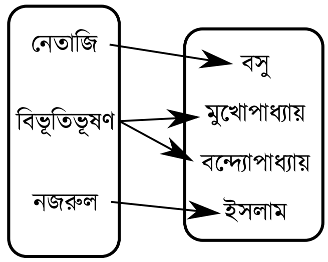


Fig 34

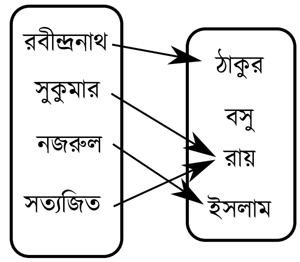


Fig 35

তীরগুলো যেমন তেমন করে আঁকলেই কিন্তু function হয় না। এমনভাবে আঁকতে হবে যেন তুমি তার ভিত্তিতে সব সময়েই নির্দ্বিধায় উত্তর দিতে পারো। কোথাও আটকে গেলে বা দ্বিধায় পড়ে গেলে হবে না। নীচের কয়েকটা উদাহরণ দেখলেই বুঝবে।

Example 28: যদি তোমাকে Fig 33-এর মত এই কয়টা নাম দিই--

{ রবীন্দ্রনাথ, নেতাজি, হরিপদ }

তবে কী করে তুমি নাম-থেকে-পদবী তীর চিহ্ন আঁকবে?
SOLUTION: প্রথম দুজনকে নিয়ে চিন্তা নেই, কিন্তু ওই "হরিপদ"-টা আবার কে রে বাবা? ওই নামে একজন সাদামাটা ছোটোখাটো লোকের অস্তিত্বের কথা শোনা যায় বটে, কিন্তু পদবীর তো উল্লেখ পাওয়া যায় না! বুঝতেই পারছ হরিপদ থেকে কোন তীর চিহ্ন আঁকা যাচ্ছে না। এই যে হোঁচট খেলে, তাই এটা আর function হল না। Function হওয়ার জন্য domain-এর প্রতিটা element থেকে তীর চিহ্ন বেরোনো চাই। ■

আরেকটা উদাহরণ দেখা যাক।

Example 29: যদি নামের set-টা এইরকম হত--

{ নেতাজি, বিভূতিভূষণ, নজরুল },

তবে তীর চিহ্নগুলো কী রকম দেখতে হত?
SOLUTION: এখানে প্রতিটি নামই পরিচিত। কিন্তু সমস্যা হবে বিভূতিভূষণকে নিয়ে। ওই নামের দুজন বিখ্যাত লোক আছেন জানি--একজন মুখোপাধ্যায়, অন্যজন বন্দ্যোপাধ্যায়। অতএব "বিভূতিভূষণ" থেকে দুটো তীর আঁকতে হচ্ছে (Fig 34)। আবার হোঁচট, খালি নাম শুনে সব সময়ে পদবীটা নির্দ্বিধায় বলা যাচ্ছে না। অতএব এটাও function নয়। Function হবার জন্য domain-এর প্রতিটা element থেকে <u>একটা</u> এবং <u>ঠিক একটাই</u> তীর চিহ্ন বেরোতে হবে। ■

এত যে কড়াকড়ি সবই কিন্তু domain-এর বেলায়, codomain-এর বেলায় এসব কোনো ঝামেলা নেই। যেমন নীচের উদাহরণে--

Example 30: ধরো নামের set-টা হল

{ রবীন্দ্রনাথ, সুকুমার, নজরুল, সত্যজিত}.

এর জন্য আমরা যদি তীর চিহ্নগুলো Fig 35-এর মত করে আঁকি তবে কি সেটা একটা function হবে?
SOLUTION: এখানে codomain-এর একটা বাড়তি পদবী রয়েছে--"বসু", যেটাতে কোনো তীর আসে নি। ওদিকে আবার "রায়" পদবীতে একাধিক তীর এসেছে। কিন্তু এগুলো আমরা গায়েই মাখব না। কারণ আমাদের কাজ হল খালি নাম শুনে পদবী বলতে পারা, এখানে তো আর সেই কাজে কখনো আমাদের হোঁচট খেতে হচ্ছে না। তাই এটা দিব্যি একটা function. ■

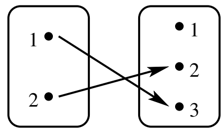


Fig 36

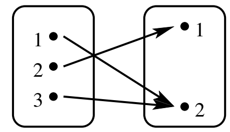


Fig 37

4.1 One-one, onto, bijection

Codomain-এর দিকে কোনো বাধা নিষেধ নেই বটে, কিন্তু কিছু বাধা নিষেধ চাপালে function-টা একটু বেশী সহজ হয়। Codomain-এর মধ্যে অব্যবহৃত element থাকতেই পারে (যেখানে কোনো তীর আসে নি)। এদের মধ্যে যদি খালি ব্যবহৃত element-গুলোর দিকে তাকাই, তবে তাদের set-টাকে বলে function-টার range. এটা আমরা আগেই শিখেছি। যেমন এক্ষুণি যে উদাহরণটা দিলাম সেখানে codomain-টা ছিল {ঠাকুর, বসু, রায়, ইসলাম}, আর range-টা ছিল {ঠাকুর, রায়, ইসলাম}.
যদি codomain-এর মধ্যে কোনো অব্যবহৃত element আদৌ না থাকে (মানে codomain=range হয়) তবে সেইরকম function-কে বলে **onto** বা **surjective.** অংকের ভাষায় সংজ্ঞাটা এরকম দেখতে--

> DEFINITION: **Onto/surjective**
>
> A function $f : A \to B$ is called **onto** or **surjective** if
>
> $$\forall b \in B \quad \exists a \in A \quad f(a) = b.$$
>
> A surjective function is also called a **surjection.**

যদি range-এর প্রতিটি element-এ ঠিক একটা করেই তীর চিহ্ন আসে, তবে সেই function-কে বলে one-one বা injective. (না, সূঁচ-ফোটানো injection-এর সঙ্গে এর কোনো সম্পর্ক নেই!)

> DEFINITION: **One-one/injective**
>
> A function $f : A \to B$ is called **one-one** or **one-to-one** or **injective** if
>
> $$\forall a_1, a_2 \in A \quad \big(f(a_1) = f(a_2) \implies a_1 = a_2\big).$$
>
> An injective function is also called an **injection**.

যদি একটা function একই সঙ্গে onto এবং one-one হয়, তাকে বলে **bijective** বা **invertible.** এখানে invertible নামটার পিছনে একটা কারণ আছে। একটা এরকম function-এর যাবতীয় তীর চিহ্নকে যদি তুমি উল্টে দাও (যাকে ইংরাজীতে বলে invert করা) তবে ফের একটা function পাবে--খালি আগের domain-টা হবে এর codomain, আর আগের codomain-টা হবে এর domain. যেহেতু invert করে ফের function পাওয়া গেল তাই নাম হয়েছে invertible অর্থাৎ যাকে ওল্টানো যায় (বা, একদম ঠিক করে বললে--যাকে উল্টে একটা function পাওয়া যায়)।

Exercise 12: Fig 36 এবং Fig 37-এ দুটো function-কে তীর চিহ্ন দিয়ে দেখানো হয়েছে। প্রথমজন onto নয়, দ্বিতীয়জন one-one নয়। এদের ওল্টালে কি ফের function পাওয়া যাবে? ■

4.2 কিছু উদাহরণ

এবার কিছু অংক করব যেখানে একটা function দেওয়া থাকবে, এবং আমাদের পরীক্ষা করে দেখতে হবে সেটা onto কিংবা one-one কিংবা bijective কিনা।

Example 31: Let S be the set of all 2×2 real symmetric matrices $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ with $ad - bc \neq 0$ and $\mathbb{R}^*$ denote the set of all nonzero real numbers. Show that the mapping $f : S \to \mathbb{R}^*$ defined as

$$f\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) = ad - bc$$

is surjective but not injective. **(1997)**

SOLUTION: প্রথমে দেখাই surjective. তার মানে $\mathbb{R}^*$-এ তুমি যাই x নাও না কেন, এমন একটা matrix A তুমি S-এর মধ্যে পাবে যাতে $f(A) = x$ হয়।

Surjective: To show:

$\forall x \in \mathbb{R}^* \quad \exists A \in S \quad f(A) = x.$

$\forall x$ Take any $x \in \mathbb{R}^*$.

তার মানে তোমাকে x দেওয়া আছে, আর তোমাকে বার করতে হবে এমন $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in S$ যাতে $ad - bc = x$ হয়। অনেকভাবে করা যায়, একটা যেমন--

$\exists A$ Choose $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} x & 0 \\ 0 & 1 \end{bmatrix} \in S.$

Then $ad - bc = x \neq 0$, as required. So f is surjective.

এবার দেখাব যে f injective নয়, অর্থাৎ S-এর মধ্যে এমন দুটো আলাদা আলাদা matrix আছে A আর B যাতে $f(A) = f(B)$ হয়। এরকম প্রচুর A, B আছে। একজোড়া এই রকম--

Injective: f is not injective because if we take $A = \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix} \in S$ and $B = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} \in S$, then $A \neq B$ but $f(A) = 2 = f(B)$.

■

Example 32: Let $f : \mathbb{N}^+ \to \mathbb{N}^+$ be the mapping given by $f(x) = 2x$, where $\mathbb{N}^+$ is the set of all positive integers. Show that f is injective but not surjective.[2] **(2000)**

SOLUTION:

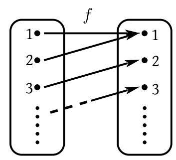


Fig 38

Injective: Shall show

$\forall m, n \in \mathbb{N}^+ \quad \big(f(m) = f(n) \implies m = n\big).$

$\forall m, n$ Take any $m, n \in \mathbb{N}^+$ with $f(m) = f(n)$.

$\because f(m) = f(n)$, $\therefore 2m = 2n$,

$\therefore m = n$, as required.

এইবার দেখাব যে, surjective নয়।

Not surjective: Shall show

$\exists y \in \mathbb{N}^+ \quad \forall n \in \mathbb{N}^+ \quad f(n) \neq y.$

এটা পেয়েছি surjective-এর সংজ্ঞার negation নিয়ে। Surjective-এর সংজ্ঞা ছিল এইরকম--

$$\forall y \in \mathbb{N}^+ \quad \exists n \in \mathbb{N}^+ \quad f(n) = y.$$

এর negation নিলে $\forall$ উল্টে $\exists$, এবং $\exists$ উল্টে $\forall$ হয়ে যাবে এবং সব শেষের $=$-টা হয়ে যাবে $\neq$.
আমাদের কাজ হল এমন একটা $y \in \mathbb{N}^+$ খুঁজে পাওয়া যেটাকে $f(n)$ মানে $2n$ আকারে লেখা যায় না। বুঝতেই পারছ যে, যা খুশী একটা odd (বিজোড়) $y \in \mathbb{N}^+$ নিলেই চলবে।

$\exists y$ Choose $y = 3 \in \mathbb{N}$.

$\forall n$ Take any $n \in \mathbb{N}^+$.

Then $f(n) = 2n$ is even, but $y = 3$ is odd. So $f(n) \neq y$, as required.

■

Example 33: Is every surjective mapping $f : \mathbb{N}^+ \to \mathbb{N}^+$ an injective mapping? Justify. ($\mathbb{N}^+$ denotes the set of all positive integers.) [3] **(2001)**

SOLUTION:

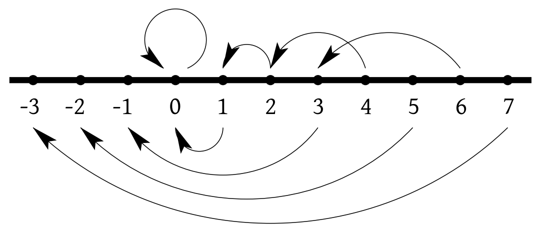


Fig 39

No, there are surjective mappings $f:\mathbb{N}^+ \to \mathbb{N}^+$ that are not injective.

For example,

$$f(n) = \begin{cases} 1 & \text{if } n = 1,2 \\ n-1 & \text{otherwise} \end{cases}$$

Fig 38-এ এই function-টাকে তীর চিহ্ন দিয়ে দেখানো হয়েছে। লক্ষ কর যে, প্রতিটি বিন্দুতেই অন্ততঃ একটা করে তীর এসেছে। সুতরাং surjective. ভালো করে দ্যাখো--প্রতিটি বিন্দুতেই একটা তীর এসেছে তার পরের বিন্দুটা থেকে। তার মানে--

Step 1: Shall show f is surjective, ie,

$\forall n \in \mathbb{N}^+ \quad \exists m \in \mathbb{N}^+ \quad f(m) = n.$

$\forall n$ Take any $n \in \mathbb{N}^+$.

$\exists m$ Choose $m = n + 1 \in \mathbb{N}^+$.

Then $m \geq 2$, and so $f(m) = m - 1 = n + 1 - 1 = n$, as required.

কিন্তু 1-এ দুটো তীর এসেছে, তাই f injective নয়--

Step 2: f is not injective, because $1 \neq 2$ but $f(1) = f(2)$.

■

Example 34: A function $f:\mathbb{Z}^* \to \mathbb{Z}$ is defined by

$$f(n) = \begin{cases} \frac{n}{2} & \text{if } n \text{ is an even integer} \\ \frac{-n+1}{2} & \text{otherwise} \end{cases}.$$

Is f injective and surjective? Here $\mathbb{Z}^*$ is the set of non-negative integers.[3] **(2003)**

SOLUTION: এরকম অংকে একটা ছবি এঁকে নিলে ভালো হয়, যেমন Fig 39-তে প্রথমে একটা লাইন ধরে ফুট্‌কি ফুট্‌কি বসিয়ে $\mathbb{Z}$ বুঝিয়েছি। 0 থেকে শুরু করে ডানদিকের অংশটা তাহলে হল $\mathbb{Z}^*$. যদি $y = f(x)$ হয়, তবে x থেকে y-তে একটা তীরচিহ্ন এঁকেছি। ভালো করে দ্যাখো তীর চিহ্নগুলো সব ঠিক হয়েছে কিনা। দুটো তীর চিহ্ন যদি একই জায়গায় যায়, তবে f injective হবে না।

Step 1: Shall show that f is not injective, ie,

$\exists m, n \in \mathbb{Z}^* \quad \big(m \neq n \text{ but } f(m) = f(n)\big).$

$\exists m, n$ Choose $m = 0 \in \mathbb{Z}^*$ and $n = 1 \in \mathbb{Z}^*$.

Then $m \neq n$ but
$$f(m) = f(0) = 0 = f(1) = f(n),$$
as required.

যদি এমন কোনো জায়গা পড়ে থাকে যেখানে কোনো তীর চিহ্ন যায় নি, তবে f-টা surjective হবে না। ছবিতে অবশ্যই আমরা পুরো $\mathbb{Z}$ দেখাই নি (দেখানো অসম্ভব, কারণ $\mathbb{Z}$-এর মধ্যে অসংখ্য point আছে)। কিন্তু যেটুকু এঁকেছি, তা থেকেই একটা প্যাটার্ণ পাওয়া যাচ্ছে। এর ভিত্তিতে আমরা দাবী করছি যে, এরকম কোনো জায়গা নেই যেখানে কোনো তীর পৌঁছোয় নি।

Step 2: Shall show f is surjective, ie,

$\forall m \in \mathbb{Z} \quad \exists n \in \mathbb{Z}^* \quad f(n) = m.$

$\forall m$ Take any $m \in \mathbb{Z}$.

এবার তীর চিহ্নগুলোর প্যাটার্ণটাকে ব্যবহার করে একটা উপযুক্ত $n \in \mathbb{Z}^*$ পেতে হবে। লক্ষ কর যে, প্রতিটি positive সংখ্যাতে তীরটা এসেছে তার দ্বিগুণের থেকে (1-এ তীর এসেছে 2 থেকে, 2-এ এসেছে 4-এর থেকে, এইরকম)। সুতরাং এটুকু বলা যায় যে প্রতিটি positive সংখ্যাই কোনো না কোনো তীরের ডগায় আছে, যেহেতু সবারই দ্বিগুণ আছে। Negative সংখ্যাদের বেলাতেও তীরগুলোর একটা প্যাটার্ণ আছে। দুয়ে মিলিয়ে বলা যায়--

$\exists n$ Choose
$$n = \begin{cases} 2m & \text{if } m \geq 0 \\ 1 - 2m & \text{otherwise} \end{cases}$$

Then if $m \geq 0$,
$$f(n) = f(2m) = \tfrac{2m}{2} = m,$$
as required. Similarly, if $m < 0$,
$$f(n) = f(1-2m) = \frac{-(1-2m)+1}{2} = m,$$
as required.

■

Example 35: Let $A = \mathbb{R} - \{-\frac{1}{2}\}$, $B = \mathbb{R} - \{\frac{1}{2}\}$, where $\mathbb{R}$ denotes the set of all real numbers. Let $f : A \to B$ be defined by
$$f(x) = \frac{x-3}{2x+1} \forall x \in A.$$

Does f^{-1} exist? Justify your answer.[3] **(2006)**

SOLUTION: এরকম অংকে $f(x)$-এর ফর্মুলাটার দিকে হাঁ করে তাকিয়ে থেকে উত্তরটা খুঁজে পাওয়ার বড় একটা আশা নেই। সুতরাং আমরা করব কি, f-টাকে হাতেকলমে ওল্টাবার চেষ্টা করব, অর্থাৎ $y = f(x)$ মানে $y = \frac{x-3}{2x+1}$ নিয়ে শুরু করে x-কে y দিয়ে প্রকাশ করার চেষ্টা করব। যদি একাজটা করা সম্ভব হয়, তবে বুঝব f-কে ওল্টানো যায়, অর্থাৎ f^{-1} exist করে। আর যদি কোথাও আটকে যাই, তবে বুঝব যে f^{-1} exist করে না।

এই কথাটা বুঝতে যদি অসুবিধা হয় তবে একটা সহজ function $g(x) = 2x$ নিয়ে পরীক্ষা করা যাক, যেখানে $g : \mathbb{R} \to \mathbb{R}$. ধরো প্রশ্ন হল g^{-1} exist করে কি না। আমরা শুরু করব $y = g(x)$ মানে $y = 2x$ নিয়ে। এটাকে উল্টে পাব $y = x/2$. যেহেতু ওল্টাতে কোনো অসুবিধা হল না, তাই g^{-1} exist করে, বস্তুতঃ $g^{-1}(y) = y/2$.

একটা function-কে ওল্টাতে কী কী অসুবিধা হতে পারত? যেমন কোথাও হয়তো শূন্য দিয়ে ভাগ এসে যেতে পারত, কিম্বা negative সংখ্যার square root বার করা। কিংবা এমনও হতে পারত যে একটা y-এর জন্য একাধিক x সম্ভব। যেমন যদি $h(x) = x^2$ নিই যেখানে $h : \mathbb{R} \to \mathbb{R}^+$, তবে $y = x^2$-কে ওল্টালে হত $x = \pm\sqrt{y}$. যেহেতু এখানে প্লাস আর মাইনাস দুটো চিহ্নই নেওয়া যায়, তাই x unique নয়। সুতরাং h^{-1} exist করে না।

অনেক আলোচনা হল, এবার মূল অংকটায় ফেরা যাক।

> Let us take $y = f(x)$ for $x \in A$ and $y \in B$. Thus,
>
> $$y = \frac{x-3}{2x+1},$$
>
> where $x \neq -\frac{1}{2}$ and $y \neq \frac{1}{2}$.

এবার আমাদের উদ্দেশ্য হল x-টাকে বাঁদিকে আনা। তার জন্য কী করতে হয় সে তো স্কুল থেকেই জানো। কয়েকটা মামূলী ধাপের পরে পাবে--

> $$x = \frac{3+y}{1-2y},$$
>
> because $y \neq \frac{1}{2}$.

এই শেষ কথাটা লেখা গুরুত্বপূর্ণ, কারণ আমরা এখানে সতর্ক লক্ষ রাখছি যে, $y = f(x)$-কে ওল্টানোর পথে কোথাও কোনো বিঘ্ন আছে কি না। যেকোনো ভাগের সময়েই তাই খেয়াল করতে হবে যেন শূন্য দিয়ে ভাগ না হয়ে যায়। এখানে $y \neq \frac{1}{2}$ দেওয়া থাকায় জোর বেঁচে গিয়েছি। যদি এটা না দেওয়া থাকত, তবে তৎক্ষণাৎ বলে দিতে পারতাম যে f^{-1} exist করে না। যুক্তি হিসেবে লিখতাম যে $f(x)$ কখনোই $\frac{1}{2}$ হতে পারে না, তাই surjective নয়।

যাই হোক আমাদের বেলায় সেসব ঝামেলা নেই, কারণ দিয়েই দিয়েছে যে $y \neq \frac{1}{2}$.

> Thus,
>
> $$\forall y \in B \quad \exists \underline{\text{unique}}\ x \in A \quad y = f(x).$$
>
> So f^{-1} exists:
>
> $$f^{-1}(y) = \frac{3+y}{1-2y}.$$

ওই "unique" শব্দটকে লক্ষ কর, ওটা কিন্তু খুব দরকারী। কী করে জানলাম যে এখানে x unique, অর্থাৎ y-এর কোনো value-র জন্য কেবল একটাই x থাকবে? কারণ আমরা equation solve করে এক্ষুণি দেখলাম যে, x-এর একটাই value বেরোলো!

এখানে "unique" কথাটা লেখার এত দরকার কেন? কারণ এতেই বোঝা যাচ্ছে যে আমাদের $f(x)$-টা injective ছিল। যদি $y = f(x)$-কে ওল্টাতে কোথাও আটকে যেতাম তবে $f(x)$-টা surjective হত না। আর যদি একাধিক x এসে যেত তবে injective হত না। তাই "unique" কথাটা বাদ দিলে খালি প্রমাণ হত যে $f(x)$ একটা surjective function. কিন্তু

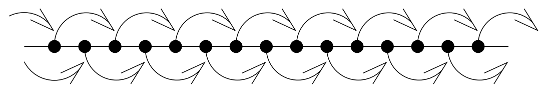


Fig 40

আমাদের দেখাতে বলেছিল যে f^{-1} exist করে, অর্থাৎ f হচ্ছে bijective. ■

Example 36: State true or false with justification: The mapping $f : \mathbb{R} \to (-1, 1)$ defined by

$$f(x) = \frac{x}{1+x^2} x \in \mathbb{R}$$

is a bijective mapping.[2] **(2005)**
SOLUTION: যথারীতি আমরা প্রথমে $y = f(x)$ নিয়ে শুরু করে সেটা থেকে x-কে y দিয়ে লেখার চেষ্টা করব। তার মানে $y = x/(1+x^2)$ অর্থাৎ $y + yx^2 - x = 0$. আমাদের কাজ হল এটাকে x-এর জন্য solve করা, y দেওয়া আছে ধরে নিয়ে। x-এর equation হিসেবে এটা একটা quadratic equation: $ax^2 + bx + c = 0$, যেখানে $a = y$, $b = -1$ আর $c = y$. আমাদের দরকার প্রতিটি y-এর জন্য যেন x বার করতে পারা। তার জন্য দরকার $b^2 - 4ac$-কে পরীক্ষা করা। যদি এটা < 0 হয়ে যায়, তবে কোনো real x-ই পাওয়া যাবে না। এখানে $b^2 - 4ac = 1 - 4y^2$. হবে। যদি ধরো $y = 1$ নিই, তবেই এটা < 0 হয়ে যাচ্ছে। সুতরাং f-টা surjective-ই হবে না! সুতরাং bijective আর হয় কী করে? ভালো করে এই জায়গাটা চিন্তা করে বুঝে নাও।
এবার গুছিয়ে লেখার পালা।

> The statement is false. Here $f(x)$ is not bijective, since it is not surjective.
>
> Actually $\nexists x \in \mathbb{R}$ such that $f(x) = 1$.
>
> Because otherwise
> $$\frac{x}{1+x^2} = 1,$$
> means
> $$x^2 - x + 1 = 0,$$
> which has no real solution since
> $$(-1)^2 - 4 \times 1 \times 1 < 0.$$

■

Example 37: State true or false with justification: The mapping $f : \mathbb{Z} \to \mathbb{Z}$ ($\mathbb{Z}$ = set of integers) defined by $f(x) = x + 2$ is not surjective.[2] **(2002)**
SOLUTION: এই অংকটায় যে ছবি আঁকা খুব গুরুত্বপূর্ণ তা নয়, কিন্তু তাও একটা এঁকেছি (Fig 40)। বোঝাই যাচ্ছে যে প্রতিটা বিন্দুতেই একটা করে তীর গিয়েছে। এখানেও ফর্মুলা ওল্টানোর কায়দাটা কাজ করবে। $y = x + 2$-কে ওল্টালে হয় $x = y - 2$. যেহেতু ওল্টাতে কোনো সমস্যা হল না, অতএব--

The statement is false. Shall show that $f(x)$ is surjective, ie,

$\forall y \in \mathbb{Z} \quad \exists x \in \mathbb{Z} \quad f(x) = y.$

$\boxed{\forall y}$ Take any $y \in \mathbb{Z}$.

$\boxed{\exists x}$ Choose $x = y - 2$.

Then

$$f(x) = x + 2 = (y - 2) + 2 = y,$$

as required.

■

Example 38: State true or false with justification: If $\mathbb{Z}^*$ is the set of all non-negative integers and $f : \mathbb{Z} \to \mathbb{Z}^*$ is defined by $f(x) = \frac{1}{2}[x + |x|]$ then $f(x)$ is a bijective mapping.[2] **(2004)**

SOLUTION: আমরা আগেই দেখেছি যে, কোনো একটা $f(x)$-এর ফর্মুলা দেওয়া থাকলে সেটা bijective কিনা দেখার একটা কায়দা হল $y = f(x)$ নিয়ে শুরু করে সেটাকে উল্টে x-কে y দিয়ে প্রকাশ করার চেষ্টা করা। আমাদের অংকে আছে $f(x) = \frac{1}{2}(x + |x|)$. তার মানে আমাদের শুরু করা উচিত $y = \frac{1}{2}(x + |x|)$ নিয়ে। কিন্তু ডানদিকে ওই $|x|$-টা থেকেই সব মাটি করে দিয়েছে, ওটাকে আবার কী করে ওল্টাবো রে বাবা!

এরকম অবস্থায় বুদ্ধিমানের কাজ হল কিছু উদাহরণ নেওয়া, বিভিন্ন x নিয়ে দেখা যে $f(x)$-গুলো কী রকম হচ্ছে। যদি কোনো দুটো আলাদা x-এ $f(x)$ একই হয়ে যায় তবে ওমনি বলে দিতে পারব যে f injective নয়। এখানে $f(1) = \frac{1}{2}(1+|1|) = 1$, $f(2) = \frac{1}{2}(2 + |2|) = 2$. এইভাবে দেখাই যাচ্ছে যে $x \geq 0$ হলে সব সময়েই $f(x) = x$ হবে। সুতরাং এখনো পর্যন্ত bijection হবার কোনো বাধা নেই। এবার তাহলে $x < 0$ নিয়ে দেখি। $f(-1) = \frac{1}{2}(-1 + |-1|) = \frac{1}{2}(-1 + 1) = 0$. একইভাবে $f(-2) = \frac{1}{2}(-2 + |-2|) = \frac{1}{2}(-2 + 2) = 0$. লক্ষ কর যে, $x < 0$ হলেই $f(x) = 0$ হচ্ছে। সুতরাং দেখাই যাচ্ছে যে f injective নয়।

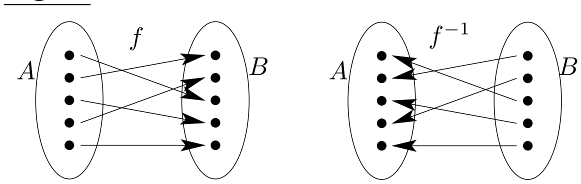
No, $f(x)$ is not bijective, because it is not injective.

For example, $f(-1) = \frac{1}{2}(-1 + |-1|) = 0$, and also $f(-2) = \frac{1}{2}(-2 + |-2|) = 0$.

Thus, $f(-1) = f(-2)$ though $-1 \neq -2$.

■

Fig 41



(a) (b)

DAY 5
Function (part 2)

একটা bijective function-কে ওল্টালে (বা invert করলে) আরেকটা নতুন function পাওয়া যায়, যাকে বলে মূল function-টার inverse function. মূল function-টাকে f বললে inverse function-টাকে বলে f^{-1}. এ সবই আমরা গতকালই শিখেছি। আজকে এই inverse function-দের নিয়ে আরেকটু গবেষণা করব।

5.1 Inverse function

Example 39: State true or false with justification: If $f : A \to B$ is invertible then $f^{-1} : B \to A$ is also invertible.[2] **(2000)**

SOLUTION: প্রথমে Fig 41 দেখে ভেবে নেওয়া যাক উত্তর কি হবে--true না false? একটা function f invertible মানে সেটা একটা bijection, যেমন (a) ছবিটাতে দেখানো হয়েছে। এখানে দুটো তীর কখনো এক জায়গায় যায় নি, সবাই আলাদা আলাদা জায়গায় পৌঁছেছে, তাই injective. আবার B-এর মধ্যে কোনো element ফাঁকা পড়ে নেই, তাই f surjective-ও বটে। একটা bijective function-কে invertible বলার কারণ এই যে, তীরগুলোকে ধরে উল্টে দিলে একটা function পাওয়া যায় $f^{-1} : B \to A$, যেমন দেখানো হয়েছে (b) ছবিটাতে।

প্রশ্ন হচ্ছে f^{-1}-এর তীরগুলোকে আবার ওল্টালে কোনো function পাওয়া যাবে কিনা। বলাই বাহুল্য যে যাবে, কারণ f-এর তীর উল্টে f^{-1}-এর তীরগুলো পেয়েছি, এখন তাদের ফের ওল্টালে আবার f-এই ফিরে যাব। সুতরাং--

> The statement is true.

এবার এই বক্তব্যটাকে অংকের ভাষায় গুছিয়ে লিখতে হবে। তীর ওল্টানোর ব্যাপারটা ছবিতে বুঝতে যত সহজ, লেখার সময়ে ততটা নয়। তাই আমরা এমনি যে ভাবে bijective দেখায় সেভাবেই এগোব, অর্থাৎ আলাদা আলাদা করে দেখাব যে, f^{-1} injective এবং surjective.

প্রথমে লিখে নিই f এবং f^{-1}-এর সম্পর্কটা ঠিক কী, অর্থাৎ একজনের তীর ওল্টালে যে অন্যজনের তীরগুলো পাওয়া যায় সেই কথাটা--

> Given: f is invertible. Thus
> $$\forall a \in A f^{-1}(f(a)) = a \quad (\mathbf{1})$$
> and
> $$\forall b \in B f(f^{-1}(b)) = b. \quad (\mathbf{2})$$

প্রথম ধাপে injective দেখাব, অর্থাৎ--

> Step 1: Shall show f^{-1} is injective, ie,
> $$\forall x, y \in B \quad \big(f^{-1}(x) = f^{-1}(y) \implies x = y\big).$$
> $\forall x, y$ Take any $x, y \in B$ with $f^{-1}(x) = f^{-1}(y)$.

এবার ওই f^{-1}-টাকে দুদিক থেকে কাটতে হবে। তার জন্য সহজ কায়দা হল দুদিকে f লাগানো--

> Applying f to both sides,
> $$f(f^{-1}(x)) = f(f^{-1}(y)),$$

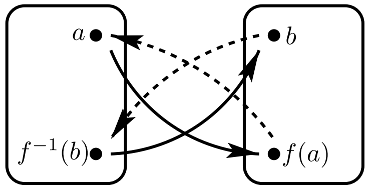


Fig 42

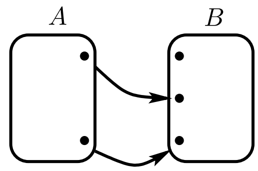


Fig 43

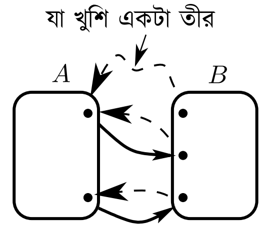


Fig 44

or, by (**2**),

$$x = y,$$

as required.

Surjective দেখানোও একই রকম ব্যাপার। প্রথমে লিখে নিই কি দেখাতে হবে--

Step 2: Shall show f^{-1} is surjective, ie,

$$\forall y \in A \quad \exists x \in B \quad f^{-1}(x) = y.$$

$\forall y$ Take any $y \in A$.

আমরা এমন x চাই যাতে $f^{-1}(x) = y$ হবে। বলাই বাহুল্য যে, $x = f(y)$ নিলেই চলবে।

$\exists x$ Choose $x = f(y) \in B$.

Then $f^{-1}(x) = f^{-1}(f(y)) = y$ by (**1**), as required.

■

এই সমাধানটার মধ্যে নীচের অংকের সমাধানটাও ঢুকে আছে।

Exercise 13: If $f : A \to B$ is a bijection then show that $\left(f^{-1}\right)^{-1} = f$. ■

Exercise 14: Let $f : A \to B$ be an invertible mapping. Then show that f^{-1} is a bijective mapping.[2] **(2009.2cii)**
HINT:
এই অংকটা Example 39-এরই রূপভেদ। ■

Exercise 15: If $f : A \to B$ is a bijective mapping, then prove that $f^{-1} : B \to A$ is also a bijective mapping.[3] **(2012.14ii)**
HINT:
আবার সেই একই জিনিস, সামান্য অন্য ভাষায়। ■

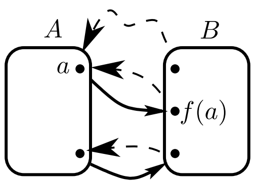


Fig 45

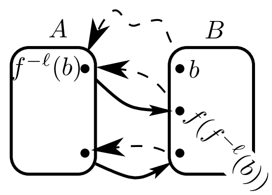


Fig 46

5.2 Left এবং right inverse

এর পর যে অংকটা করব সেখানে একটা নতুন কথা দেখবে--"left inverse". সেটা কী ব্যাপার না বুঝলে অংকটা করা যাবে না। আমরা আগেই বলেছি যে, f যদি একটা bijection হয় তবে তাকে invert করলে (মানে তীর চিহ্নগুলোকে ওল্টালে) একটা নতুন function পাওয়া যায়, যাকে আমরা f^{-1} বলি। এবার Fig 42 লক্ষ কর। তুমি যদি কোনো $a \in A$ নিয়ে শুরু করে প্রথমে f এবং তারপর f^{-1} লাগাও, তবে আবার a-তেই ফিরে আসবে, মানে

$$\forall a \in A \quad f^{-1}(f(a)) = a.$$

আবার যদি কোনো $b \in B$ নিয়ে শুরু করতে, তবে প্রথমে f^{-1} এবং তারপরে f লাগালে ফের b-তেই ফিরে আসবে, মানে--

$$\forall b \in B \quad f(f^{-1}(b)) = b.$$

এই দুটো জিনিসকে এভাবে ভাবতে পারো--f-এর বাঁদিকে বা ডানদিকে যেদিকেই f^{-1} লাগাই না কেন, সেটা f-এর সঙ্গে কাটাকাটি হয়ে যায়।
এবার ধরো এমন একটা $f : A \to B$ নিয়ে শুরু করলাম যেটা one-one কিন্তু onto নয় (Fig 43)। তাহলে তীর চিহ্নগুলো সব ওল্টালে ব্যাপারটা আর function থাকবে না, কারণ B-এর কোনো কোনো element থেকে কোনো তীর বেরোবে না। কিন্তু সেটাকে আমরা এড়াতে পারি এইভাবে-- এই সব অব্যবহৃত element থেকে যা খুশী একটা তীর টেনে দেব A-র কোনো element-এ। Fig 44 দ্যাখো। তাতে আমরা একটা function পাব। এটাকে বলে f-এর একটা left inverse. একে অনেকসময়ে লেখা হয় $f^{-\ell}$. কেন "একটা" বললাম বুঝতেই পারছ, বাড়তি "যা খুশী" তীরগুলো কীভাবে এঁকেছি তার উপর নির্ভর করে আরও অনেক left inverse হতে পারে। এটাকে "left" inverse কেন বলে, সেটা বোঝা কঠিন নয়। মনে কর যে কোনো $a \in A$ নিলাম। যদি এবার প্রথমে f এবং তারপর $f^{-\ell}$ লাগাই তবে আবার a-তেই ফিরব (Fig 45), অর্থাৎ

$$\forall a \in A \quad f^{-\ell}(f(a)) = a.$$

লক্ষ কর যে, এই কাজে বাড়তি "যা খুশী" তীরগুলো কোনো ভূমিকা পালন করছে না। কিন্তু যদি যে কোনো $b \in B$ নিয়ে শুরু করি, তবে প্রথমে $f^{-\ell}$ এবং তারপরে f লাগালে b-তে নাও ফিরে আসতে পারি। একটা এরকম উদাহরণ রয়েছে Fig 46-এ। তাই এখানে বলা যায় যেন f-এর বাঁদিকে $f^{-\ell}$ লাগালে কাটাকাটি হয়, কিন্তু ডানদিকে লাগালে নাও হতে পারে। সেই কারণেই "left" inverse নাম।

Example 40: A function $f : \mathbb{Z} \to \mathbb{Z}$ is defined by

$$f(x) = \begin{cases} \frac{x}{2} & \text{if } x \text{ is even} \\ 7 & \text{if } x \text{ is odd} \end{cases}$$

Find a left inverse of f, if it exists.[2] **(2010.2cii)**
SOLUTION: চট্ করে দেখে নিই function-টা one-one কিনা। কারণ একমাত্র তাহলেই left inverse থাকবে।

> This function is not one-one, since $f(1) = f(3) = 7$ but $1 \neq 3$.

সুতরাং মনে মনে বুঝে গেছি যে, left inverse-এর কোনো আশা নেই। এবার সেটা প্রমাণ করব।

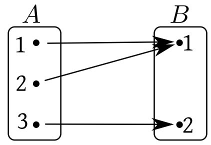


Fig 47

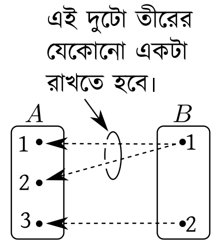


Fig 48

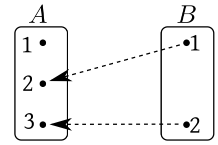


Fig 49

> Let, if possible, f have a left inverse $f^{-\ell}$. Then we must have
>
> $$\forall n \in \mathbb{Z} \quad f^{-\ell}(f(n)) = n.$$
>
> Putting $n = 1, 3$ we have
>
> $$f^{-\ell}(f(1)) = 1 \text{ and } f^{-\ell}(f(3)) = 3.$$
>
> So $f^{-\ell}(7) = 1$ and $f^{-\ell}(7) = 3$.

কিন্তু $f^{-\ell}$-কে তো একটা function হতে হবে। সুতরাং $f^{-\ell}(7)$ একই সঙ্গে 1 এবং 3 দুটোই তো হতে পারে না!

> So $f^{-\ell}$ cannot be a function ($\Rightarrow\Leftarrow$).

■

এই অংকের সমাধানটা ভালো করে পড়ে নাও। তারপর নীচের অংকটা কর।

Exercise 16: Let $f : A \to B$ be any function with a left inverse. Show that f must be one-one. ■

Left inverse বলে যদি একটা জিনিস হয়, তবে right inverse বলেই বা হবে না কেন? সেই জিনিসটা এইরকম--

সজারু, ক্যাঙারু, দেবদারু সব হতে পারে, মজারু কেন হবে না?
--সুকুমার রায়

ধরো এমন একটা $f : A \to B$ নিয়ে শুরু করলাম যেটা onto, কিন্তু one-one নয় (Fig 47)। তাহলে তীর চিহ্নগুলো সব ওল্টালে ব্যাপারটা আর function থাকবে না, কারণ B-এর কোনো কোনো element থেকে একাধিক তীর বেরোবে। কিন্তু সেটাকে আমরা এড়াতে পারি এইভাবে-- যেই দেখব একটা element থেকে একাধিক তীর বেরিয়েছে, অমনি তাদের মধ্যে খালি একটাকে রাখব (যেকোনো একটা, যেটা খুশী), আর বাকিগুলোকে মুছে ফেলব। Fig 48 দ্যাখো। তাতে আমরা Fig 49-এর মত একটা function পাব। এটাকে বলে f-এর একটা right inverse. কেন "একটা" বললাম বুঝতেই পারছ, কোন তীরগুলো মুছেছি আর কোন তীরগুলো রেখেছি তার উপর নির্ভর করে আরও অনেক right inverse হতে পারে। এটাকে "right" inverse কেন বলে সেটা ছবি এঁকে বোঝা কঠিন নয় (চেষ্টা করে দ্যাখো!)।

Exercise 17: Let $f : A \to B$ be a function with a right inverse. Show that f must be onto. ■

যদি সবকিছু পড়তে গিয়ে মাথা গুলিয়ে গিয়ে থাকে তাই গুছিয়ে লিখে নিই।

DEFINITION: Left inverse

Let $f : A \to B$ be any function. A function $g : B \to A$ is called a **left inverse** of f if

$$\forall a \in A \quad g(f(a)) = a.$$

DEFINITION: Right inverse

Let $f : A \to B$ be any function. A function $g : B \to A$ is called a **right inverse** of f if

$$\forall b \in B \quad f(g(b)) = b.$$

কোনো function-এর left বা right inverse কখন থাকে? তার উত্তর হল--

- কোনো function যদি one-one হয়, তবে (এবং একমাত্র তবেই) তার left inverse থাকবে।
- কোনো function যদি onto হয়, তবে (এবং একমাত্র তবেই) তার right inverse থাকবে।
- কোনো function যদি একইসঙ্গে one-one এবং onto হয়, তবে (এবং একমাত্র তবেই) তার inverse থাকবে। এই inverse-টাই হবে একাধারে ওর left এবং right inverse.

এবার কয়েকটা অংক দিই যেগুলো মোটেই কঠিন নয় কিন্তু, বেশ দরকারী। ছবি দিয়ে বুঝতে তো খুবই সহজ, অংকের ভাষায় লিখে প্রমাণ করাও কঠিন কিছু নয়।
আমরা আগেই দেখেছি যে, যদি $f : A \to B$ একটা bijection হয় তবে $f^{-1} : B \to A$-ও একটা bijection হতে বাধ্য। শুধু তাই নয়, f^{-1}-এর inverse-টা আবার f স্বয়ং, মানে $\left(f^{-1}\right)^{-1} = f$.
কতকটা একইরকম কথা বলা চলে left এবং right inverse-দের সম্পর্কেও। সেটা নিয়েই নীচের অংক দুটো।

Exercise 18: Let $f : A \to B$ be a one-one function with a left inverse $f^{-\ell} : B \to A$. Show that $f^{-\ell}$ must be an onto function, and $\left(f^{-\ell}\right)^{-r} = f$. ■

Exercise 19: Let $f : A \to B$ be a onto function with a right inverse $f^{-r} : B \to A$. Show that f^{-r} must be a one-one function, and $\left(f^{-r}\right)^{-\ell} = f$. ■

Fig 50

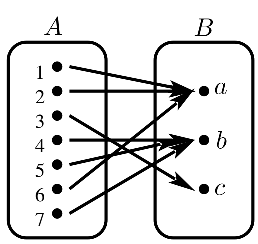
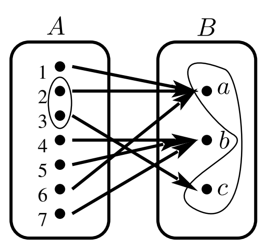


Fig 51



এবার দুটো ঠকানো প্রশ্ন দিই। ছবি না আঁকলে মুস্কিলে পড়বে সেটা আগেভাগেই বলে দিচ্ছি!

Exercise 20: এমন A, B এবং $f : A \to B$ কি সম্ভব যাতে f-টা one-one কিন্তু onto নয়, অথচ ওর ঠিক একটাই left inverse আছে? ■

নীচের অংকটাও একই সুরের।

Exercise 21: এমন A, B আর $f : A \to B$ কি সম্ভব যাতে f-টা onto কিন্তু one-one নয়, অথচ ওর ঠিক একটাই right inverse আছে? ■

DAY 6
Function (part 3)

6.1 Image of a set

ধরো একটা function দিলাম Fig 50-এর মত। যদি জানতে চাই $f(\{2,3\})$ কী হবে, তবে তুমি হয়তো খাবি খাবে, কারণ $f(2)$ বা $f(3)$ মানে কী সেটা জানি, কিন্তু f-এর পেটের মধ্যে আস্ত একটা set $\{2,3\}$ ঢুকিয়ে দেওয়া তো এখনও এ বইতে আমরা দেখি নি! এটা অংকের জগতে একটা বহুল প্রচলিত notation. এর মানে হল 2 আর 3 থেকে যে তীর বেরিয়েছে তারা কোথায় কোথায় পৌঁছেছে তাদের set. অর্থাৎ

$$f(\{2,3\}) = \{f(2), f(3)\}.$$

Fig 51 দ্যাখো। আমরা $f(\{2,3\})$-কে বলি image of $\{2,3\}$ under f. সংজ্ঞাটা আমরা এইভাবে লিখতে পারি--

DEFINITION: **Image of a set**

Let $f : A \to B$ be any function. Let $S \subseteq A$. Then the **image** of S under f is defined as the set $f(S) \subseteq B$, where

$$f(S) = \{f(x) \ : \ x \in S\}.$$

Exercise 22: ধরো f একটা function যার domain হল A এবং codomain হল B. তবে $f(A)$ হবে B-এর একটা subset. এই set-টার একটা বিশেষ নাম আছে যেটা আমরা এই বইতে আগেই শিখেছি। কি সেই নাম? ■

একটা function-এর domain-এর subset-দের নিয়ে নাড়াচাড়া করলে image-গুলো কীভাবে codomain-এর ভিতর নড়েচড়ে, সেটা বোঝাটা অনেক সময়েই খুব কাজে লাগে। এই নিয়েই নীচের অংকগুলো।
প্রথমে দেখি দুটো set-এর intersection নিলে তাদের image-গুলোরও intersection হয় কিনা। নীচের অংকটা বলছে যে f যদি one-one হয়, তবে অন্ততঃ সেটা হয়।

Example 41: $f : A \to B$ is an injective mapping from a set A into the set B. If C, D are subsets of A, then prove that

$$f(C \cap D) = f(C) \cap f(D).$$

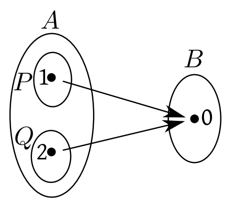


Fig 52

[3] **(1999)**

SOLUTION: দুটো set $f(C \cap D)$ আর $f(C) \cap f(D)$-কে সমান দেখাতে হবে, তার মানে দুটো জিনিস দেখালেই চলবে $f(C \cap D) \subseteq f(C) \cap f(D)$ আর $f(C) \cap f(D) \subseteq f(C \cap D)$
দুই ধাপে দুটো দেখাব।

> Step 1: Shall show $f(C \cap D) \subseteq f(C) \cap f(D)$.

তার মানে দেখাব যে, $f(C \cap D)$-এর যে কোনো element $f(C) \cap f(D)$-এর মধ্যেও আছে।

> Take any $y \in f(C \cap D)$.
>
> Then $y = f(x)$ for some $x \in C \cap D$.
>
> Since $x \in C$, so $y \in f(C)$.
>
> Since $x \in D$, so $y \in f(D)$.So $y \in f(C) \cap f(D)$, as required.

এখনও পর্যন্ত f যে injective সেটা লাগেনি। এবার অন্য দিকটা, এখানে f-এর injective-এর হওয়াটা জরুরী।

> Step 2: Shall show that $f(C) \cap f(D) \subseteq f(C \cap D)$.
>
> Take any $y \in f(C) \cap f(D)$.
>
> Since $y \in f(C)$, so $y = f(x_1)$ for some $x_1 \in C$.
>
> Since $y \in f(D)$, so $y = f(x_2)$ for some $x_2 \in D$. Thus, $f(x_1) = y = f(x_2)$.

যেহেতু f injective সুতরাং $f(x_1) = f(x_2)$ হওয়া মানে $x_1 = x_2$ হতে বাধ্য।

> Since f is injective, this means
>
> $$x_1 = x_2 = x, \text{ say.}$$

তার মানে x-টা একাধারে C এবং D দুটোতেই আছে।

> Then $x \in C \cap D$. So $y = f(x) \in f(C \cap D)$, as required.

■

যদি f-টা one-one হয়, তবে দুটো set-এর intersection-এর image পাওয়া যায় image দুটোর intersection নিলেই। এক্ষুণি যে অংকটা করলাম সেখান থেকে এটুকু শিক্ষালাভ করা গেল। কিন্তু যদি f-টা one-one না হত? তবে ব্যাপারটা সুবিধার নাও হতে পারে। নীচের অংকে সেটা দেখাতে বলেছে।

Example 42: Let $f : A \to B$ be a mapping and P, Q be two nonempty subsets of A. Give an example where

$$f(P \cap Q) \neq f(P) \cap f(Q).$$

[2] **(2004)**

SOLUTION: এখানে একটা counter example বানাতে হবে। এটা বানানো কিছুটা সহজ হবে যদি আগের অংকটা তোমার মাথায় থাকে, যেখানে আমরা দেখিয়েছিলাম যে f injective হলে $f(P \cap Q) = f(P) \cap f(Q)$ হয়। সুতরাং counterexample-এ আর যাই হোক injective f নিলে চলবে না। Counterexample বানাবার জন্য ছবি এঁকে নেওয়া প্রায়শঃই সুবিধাজনক। এমন একটা function-এর ছবি আঁকতে চাই যেটা injective নয়, তাই দুটো তীর এঁকে শুরু করেছি যারা একই জায়গায় যায় (Fig 52)। খানিকক্ষণ মাথা চুলকে একটা P আর Q-ও খাড়া করা গিয়েছে--

> An example where $f(P \cap Q) \neq f(P) \cap f(Q)$:
> Let $A = \{1, 2\}$, $B = \{0\}$ and $f(1) = f(2) = 0$. If we take $P = \{1\}, Q = \{2\}$
> then $f(P) = f(Q) = \{0\}$.

সাবধান, $f(P)$ কিন্তু $\{0\}$, খালি 0 নয়!

> So $f(P) \cap f(Q) = \{0\}$.
> But $f(P \cap Q) = f(\phi) = \phi \neq \{0\}$.

■

Example 43: State true or false with justification: If $f : X \to Y$ is a mapping and A, B are subsets of X, then $f(A \cap B) = f(A) \cap f(B)$.[2] **(1997)**

SOLUTION:

> The statement is false.

একটা counterexample আগের অংকেই দিলাম। ■

সুতরাং দেখা যাচ্ছে যে, দুটো set-এর intersection-এর image সব সময়ে image-দুটোর intersection নাও হতে পারে। সেটা হবেই যদি function-টা one-one হয়। কিন্তু এবার দেখব যে, union-এর ক্ষেত্রে ব্যাপারটা বেশী সুবিধাজনক--যদি দুটো set-এর union নাও, তবে কিন্তু image-গুলোরও union হবে! এবং তার জন্য one-one বা অন্য কোনো শর্ত লাগবে না।

Example 44: Let $f : A \to B$ be a mapping and P, Q be two nonempty subsets of A. Show that $f(P \cup Q) = f(P) \cup f(Q)$.[3] **(2004,2014)**

SOLUTION: প্রথমেই বলে রাখি--এখানে P, Q-এর nonempty হওয়ার কোনো দরকার নেই। দেখাতে হবে যে, দুটো set $f(P \cup Q)$ আর $f(P) \cup f(Q)$ সমান। তার মানে দুই ধাপে দেখাতে হবে

$$f(P \cup Q) \subseteq f(P) \cup f(Q) \text{ আর } f(P) \cup f(Q) \subseteq f(P \cup Q).$$

> Step 1: Shall show $f(P\cup Q)\subseteq f(P)\cup f(Q)$:
> Take any $b\in f(P\cup Q)$.
> Then $b=f(a)$ for some $a\in P\cup Q$.

যেহেতু $a\in P\cup Q$, সুতরাং হয় $a\in P$ আর নয়তো $a\in Q$.

> If $a\in P$, then $b=f(a)\in f(P)$.
> If $a\in Q$, then $b=f(a)\in f(Q)$.
> So in both cases we must have $b\in f(P)\cup f(Q)$.
> Thus $f(P\cup Q)\subseteq f(P)\cup f(Q)$.

এবার পরের ধাপ--

> Step 2: Shall show $f(P)\cup f(Q)\subseteq f(P\cup Q)$:
> Take any $b\in f(P)\cup f(Q)$.
> Then either $b\in f(P)$ or $b\in f(Q)$.
> If $b\in f(P)$, then $b=f(a)$ for some $a\in P$.
> If $b\in f(Q)$, then $b=f(a)$ for some $a\in Q$.
> So in both cases we must have
> $b=f(a)$ for some $a\in P\cup Q$.
> Thus $f(P)\cup f(Q)\subseteq f(P\cup Q)$.

ছোট্টো করে একটা উপসংহার টেনে দিই--

> Hence we have $f(P\cup Q)=f(P)\cup f(Q)$, as required.

■

আমরা union এবং intersection নিয়ে আলোচনা করলাম। তবে complement-ই বা বাদ থাকে কেন? সুতরাং নীচের অংকটা করেই ফ্যালো।

Exercise 23: Let $f:A\to B$ be a function. Let $S\subseteq A$. Then show that it is possible to have $f(S^c)\neq f(S)^c$.
HINT: এখানে S^c মানে $A\setminus S$, আর $f(S)^c$ মানে $B\setminus f(S)$. আগের অংকের counterexample-টাকেই একটু কায়দা করে ব্যবহার কর। ■

হুম্‌ম্‌, সুতরাং দ্যাখা যাচ্ছে যে, union-টাই একমাত্র ভদ্র আচরণ করছে, intersection আর complement দুজনেই মুস্কিলের। আচ্ছা, intersection-কে তো আমরা শায়েস্তা করেছিলাম f-কে one-one নিয়ে। Complement-এর বেলাতেও সেরকম কিছু করা যায় না? এবারের অংকটা তোমাকে সেই গবেষণাটাই করতে বলছে।

Exercise 24: ধরো $f:A\to B$ একটা function, আর $S\subseteq A$. এবার f-এর উপর নীচের কোন শর্তটা চাপালে নিশ্চিন্তে সব সময়ে বলা যাবে যে $f(S^c)=f(S)^c$ হবেই?

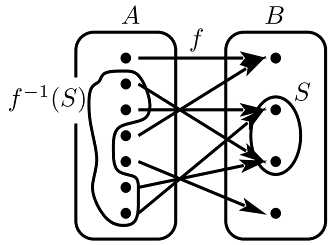


Fig 53

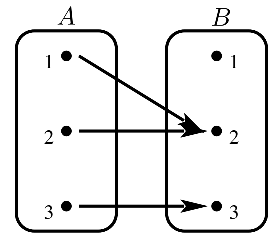


Fig 54

(1) one-one? **(2)** onto? **(3)** bijection? **(4)** নাকি কোনোটাই নয়? ■

এবার গবেষণাটাকে আরেক ধাপ এগিয়ে নিয়ে নীচের অংকটা করার চেষ্টা কর। এটা সামান্য শক্ত, contradiction দিয়ে ভাবলে হয়তো সুবিধা হবে।

Exercise 25: আবার একটা $f : A \to B$ নিয়ে শুরু করি। ধরো f-টা এত সুন্দর যে, যাই $S \subseteq A$ তুমি নাও না কেন, সব সময়েই $f(S^c) = f(S)^c$ হবে। তাহলে কি জোর দিয়ে বলা যায় যে f-টা একটা bijection হবেই? ■

যদি এইরকম গবেষণা করতে তোমার ভালো লাগে, তবে নিজে নিজেই এরকম বিস্তর অংক বানাতে পারো। যেমন ধরো $f : A \to B$ নিয়ে শুরু করলে। A-র মধ্যে দুটো subset নিলে S_1, S_2. এবার নিজেকেই প্রশ্ন করলে

"$f(S_1 \setminus S_2) = f(S_1) \setminus f(S_2)$ কি হবেই?"

যদি প্রমাণ হল তো ভালো। নইলে counterexample খুঁজলে। তারপর পরীক্ষা করে দেখতে পারো যে বাড়তি কী কী শর্ত চাপালে এটা হয়। এবং সবচেয়ে কম কতটুকু শর্ত দিয়ে কাজটা সেরে ফেলা যায়। শুনলে হয়তো আশ্চর্য লাগবে, আসলে বড় বড় গণিতজ্ঞরা কিন্তু ঠিক এইভাবেই গবেষণা করেন। অবশ্য তাঁদের হাতে বিস্তর সময় থাকে, পরীক্ষার তাড়া থাকে না তো!

6.2 Preimage of a set

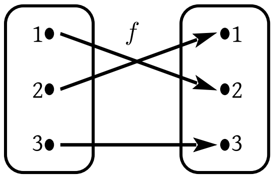
আমরা image নিয়ে অনেক গবেষণা করলাম। এই প্রসঙ্গে একইরকম আরেকটা জিনিসের কথা না বললেই নয়। জিনিসটার নাম **preimage.** ব্যাপারটা image-এর কতকটা উল্টো জিনিস। ধরো $f : A \to B$ একটা function. আমরা image-এর বেলায় A-র একটা subset নিয়ে শুরু করেছিলাম, এবার শুরু করব B-এর subset নিয়ে--$S \subseteq B$. তাহলে S-এর preimage হবে A-র একটা subset, যেটাকে লিখব $f^{-1}(S)$. সংজ্ঞাটা এইরকম--

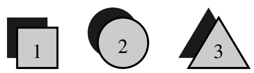
DEFINITION: Preimage of a set

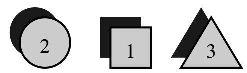
Let $f : A \to B$ and $S \subseteq B$. Then the **preimage** of S under f is defined as the set $f^{-1}(S) \subseteq A$, where

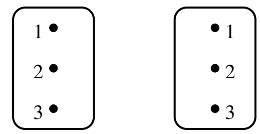
$$f^{-1}(S) = \{a \in A \ : \ f(a) \in S\}.$$

ছবি দিয়ে ভাবতে চাইলে Fig 53 দ্যাখো। S-এর প্রত্যেকটা element-এ যে সব তীর এসেছে তাদের গোড়াগুলো নিয়ে $f^{-1}(S)$ তৈরী। Preimage-এর notation-টা নিয়ে অনেক ছাত্র খাবি খায়। f^{-1} তো f-এর inverse বোঝায়, কিন্তু f যদি bijection না হয় তবে তো তার inverse থাকবে না, তাহলে সংজ্ঞাটাতে f-কে bijection ধরলাম না কেন?
এই অতি সঙ্গত প্রশ্নের উত্তর হল--এখানে আসলে একই চিহ্ন f^{-1} দিয়ে দুটো আলাদা জিনিস বোঝানো হচ্ছে। যদি f^{-1}-এর পেটে B-এর খালি একটা element থাকে তবে f^{-1} মানে f-এর inverse, এবং তার জন্য f-কে bijective হতে হবে।


Fig 55


Fig 56


Fig 57


Fig 58

কিন্তু f^{-1}-এর পেটে যদি B-এর কোনো subset দ্যাখো, তবে বুঝবে যে preimage-এর কথা হচ্ছে, এবং তার জন্য কোনো bijection-এর দরকার নেই। একটা উদাহরণ দেখলে বুঝতে সুবিধা হবে।

Example 45: ধরো Fig 54-এর function-টা নিলাম। বল তো $f^{-1}(2)$ আর $f^{-1}(\{2\})$ কী কী হবে!

SOLUTION: এখানে $2 \in B$ এবং $\{2\} \subseteq B$. সুতরাং $f^{-1}(2)$ বার করার জন্য আমরা প্রথমে f-এর inverse বার করতে চাইব। কিন্তু f-টা এখানে bijective নয় (কারণ one-one নয়)। তাই $f^{-1}(2)$ হবে undefined.
কিন্তু $f^{-1}(\{2\})$-এর বেলায় সে সব কোনো সমস্যা নেই, তাই $f^{-1}(\{2\}) = \{1, 2\}$ হবে। ■

Exercise 26: বল তো Fig 54-তে $f^{-1}(\{1\})$ কি হবে! ■

Notation-এর দিক দিয়ে preimage জিনিসটা একটু বদখত্ হলেও আসলে কিন্তু এটা image-এর চেয়েও ভালো। Image-এর বেলায় দেখেছিলাম যে খালি union-এর আচরণ ভদ্র, intersection, complement দুজনেই ঝামেলা করে। কিন্তু preimage-এর কাছে ওরা সবাই ঠাণ্ডা। সেটাই হল নীচের অংকটার বক্তব্য।

Exercise 27: Let $f : A \to B$ and $S_1, S_2, S \subseteq B$. Then prove that

1. $f^{-1}(S_1 \cup S_2) = f^{-1}(S_1) \cup f^{-1}(S_2)$,
2. $f^{-1}(S_1 \cap S_2) = f^{-1}(S_1) \cap f^{-1}(S_2)$,
3. $f^{-1}(S^c) = \left(f^{-1}(S)\right)^c$.

■

এই জন্যেই notation-টা সামান্য কঠিন হওয়া সত্ত্বেও অংকের জগতে image-এর ব্যবহারের চেয়ে preimage-এর ব্যবহার অনেক বেশী। ট্রেনে যাবার সময়ে একজন হকারকে প্রায়ই চ্যবনপ্রাশ ফেরী করতে দেখি। তার সঙ্গে সুর মিলিয়ে preimage-এর গুণ গাওয়া চলে--

> এটা দেখতে কালো, কিন্তু খেতে ভালো!

6.3 Finite set-এর মজা

আমরা নানা ধরণের function-এর কথা শিখেছি--onto, one-one এবং দুয়ে মিলে bijection. একটা function যদি bijective হয়, তবে ওরা অবশ্যই one-one এবং onto হতে বাধ্য। কিন্তু আমরা এরকম অনেক উদাহরণ দেখেছি যেখানে একটা function হয়তো onto কিন্তু one-one নয়, বা one-one কিন্তু onto নয়। এইবার আমরা একটা বিশেষ ধরণের function নিয়ে কাজ করব যাদের ক্ষেত্রে onto, one-one এবং bijection আসলে সমার্থক! অর্থাৎ এই ধরণের function-দের কারোর যদি এই তিনটের মধ্যে একটা গুণও থাকে, তবে তার বাকি দুটো গুণও থাকতে বাধ্য। এই বিশেষ ধরণের

function-রা হল $f : S \to S$ যেখানে S একটা finite set. বস্তুতঃ $f : S \to T$ হলেও আপত্তি নেই, যদি S এবং T সমান সাইজের finite set হয়। আমরা উদাহরণ দেবার সময়ে অবশ্য $S = T$ ধরে নেব।
প্রথমে একটু গা গরম করে নিই নীচের অংকটা দিয়ে।

Example 46: Find all bijective mappings from the set A onto itself where $A = \{1, 2, 3\}$.[3] **(1998)**

SOLUTION: একটু ছবি এঁকে ভাবি (Fig 55)। এখানে $f(1) = 2, f(2) = 1, f(3) = 3$. এটাকে এইভাবে ভাবতে পারো--1 যাচ্ছে 2-এ, 2 যাচ্ছে 1-এ, আর 3 থাকছে 3-এই। ঠিক যেন তোমাকে তিনটে জিনিস সাজাতে দিয়েছে, যাদের গায় $1, 2, 3$ সংখ্যা লেখা আছে (Fig 56)। তুমি 1 নম্বরকে রাখছ 2 নম্বরের জায়গায়, 2 নম্বরকে 1 নম্বরের জায়গায় এবং 3 নম্বরকে যথাস্থানে রেখে দিচ্ছ (Fig 57)। সুতরাং একটা bijection মানে হল জিনিসগুলোকে কোনোভাবে সাজানো। আমরা জানি যে 3-টে জিনিসকে মোট $3! = 6$-ভাবে সাজানো যায়, সুতরাং মোট bijection-ও পাওয়া যাবে ঠিক ততগুলোই।

> There are exactly $3! = 6$ bijective mappings from A to A:
>
> $$\begin{array}{lll} 1 \mapsto 1 & 2 \mapsto 2 & 3 \mapsto 3, \\ 1 \mapsto 1 & 2 \mapsto 3 & 3 \mapsto 2, \\ 1 \mapsto 2 & 2 \mapsto 1 & 3 \mapsto 3, \\ 1 \mapsto 2 & 2 \mapsto 3 & 3 \mapsto 1, \\ 1 \mapsto 3 & 2 \mapsto 1 & 3 \mapsto 2, \\ 1 \mapsto 3 & 2 \mapsto 2 & 3 \mapsto 1. \end{array}$$

এই "$\mapsto$" চিহ্নটাকে লক্ষ কর। এটা কোনো function লেখার একটা কায়দা, যেমন এই তালিকার প্রথম function-টা হল f যেখানে $f(1) = 1, \quad f(2) = 2$ আর $f(3) = 3$. অর্থাৎ $f(x) = y$ না লিখে $x \mapsto y$ লেখা একই ব্যাপার। তবে "$\mapsto$" দিয়ে লেখার সুবিধা হল function-টার আলাদা করে কোনো নাম দিতে হয় না। ■

এবার একটা ছোট্টো জিনিস আঁকার চেষ্টা করা যাক। Fig 58-এ এমনভাবে তীর চিহ্ন আঁকো যাতে একটা one-one function তৈরী হয়, যেটা bijective নয়। একটু চেষ্টা করলেই বুঝবে যে, সেটা সম্ভব নয়, কারণ যেহেতু function, সুতরাং domain-এর প্রতিটা বিন্দু থেকেই ঠিক একটা করে তীর চিহ্ন আঁকতে হবে। যেহেতু one-one, তাই তীর চিহ্নগুলোকে codomain-এর আলাদা আলাদা বিন্দুতে যেতে হবে। সুতরাং এতেই codomain-এর তিনটে বিন্দু খরচা হয়ে যাচ্ছে, অতএব onto না হয়ে পথ নেই, সুতরাং bijection-ও হতেই হবে।
একই রকম যুক্তি খাটত যদি একটা onto function আঁকার চেষ্টা করতে-- তোমার হাতে আছে মোটে তিনটে তীর, তা দিয়ে codomain-এর তিনটে বিন্দুকেই যদি ব্যবহার করতে হয়, তবে বিন্দু-পিছু খালি একটা করেই তীর বরাদ্দ করা যাবে। অতএব one-one (এবং তাই bijective) হওয়া কেউ ঠেকাতে পারে না।
বুঝতেই পারছ যে, এই যুক্তি শুধু $\{1, 2, 3\}$-ই নয়, যে কোনো finite set-এর বেলাতেই খাটে। এইটাই নীচের অংকে প্রমাণ করতে বলেছে।

Example 47: Let S be a finite set and let $f : S \to S$. If f is one-to-one then show that f is onto. Examine whether this remains true if the set S is infinite. **(2008)**

SOLUTION:

> By definition f is onto $f(S)$.

$f(S)$ কাকে বলে মনে আছে নিশ্চয়ই? আমরা যদি f-কে তীর চিহ্ন দিয়ে ভাবি, তবে যেসব বিন্দুতে তীর পৌঁছেছে খালি তাদের set -টাকেই $f(S)$ বলে, যার আরেকটা নাম হল f-এর range.

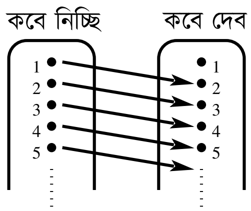


Fig 59

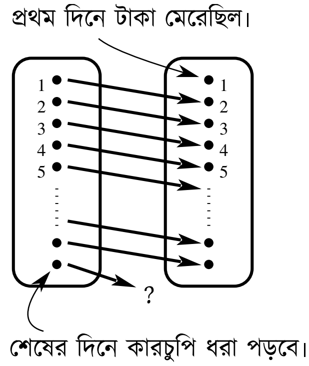


Fig 60

বুঝতেই পারছ যে, $f(S)$-এর প্রতিটি বিন্দুতেই অন্ততঃ একটা করে তীর পৌঁছতে বাধ্য, কারণ সেইভাবেই তো $f(S)$-টা তৈরী করা হয়েছে। সুতরাং f-কে যদি S থেকে $f(S)$-এ একটা function হিসেবে দেখি, তবে বলাই বাহুল্য যে, সেটা একটা onto function হতে বাধ্য। এই কথাটাই লেখা হয়েছে।
এদিকে f তো one-one বলা ছিলই। অতএব--

> So f is a bijection from S to $f(S)$.

দুটো set-এর মধ্যে একটা bijection থাকা মানে ওদের সাইজ সমান--

> Hence $|S| = |f(S)|$.

এখানে $|S|$ বলতে S-র সাইজ বোঝানো হয়েছে। এদিকে S তো একটা finite set, তার ভিতর $f(S)$ একটা subset. যদি subset-টার সাইজ মূল set-টার সমানই হয়ে গেল, তবে আর বাকী থাকল কী? তার মানে subset-টা আসলে পুরো set-টাই জুড়ে আছে!

> Since $f(S) \subseteq S$, so
> $$|S - f(S)| = |S| - |f(S)| = 0,$$
> since S is finite.
> Thus, $S = f(S)$.
> Hence f is onto S, as required.

এই যুক্তিতে S-র finite হওয়াটা জরুরী। কারণ নইলে ওই $|S| - |f(S)|$ জিনিসটা $\infty - \infty$ হয়ে ঝামেলা পাকাত। বস্তুতঃ $|S| = \infty$ হলে result-টা true নয়। পরের অংশে এটাই আমাদের দেখাতে বলা হয়েছে--

> No, this result is not true if $|S| = \infty$.

মনে রেখো যে "$\infty - \infty$ তো undefined সুতরাং result-টা এক্ষেত্রে true হতে পারে না" এই কথা বলে ছেড়ে দিলেই চলবে না। এখানে একটা counter example দিতে হবে--

Counterexample: If $S=\mathbb{N}$ then $f:S\to S$ defined as $f(x)=2x$ is one-one

⟦ Because:

$$2x=2y \implies x=y.$$

⟧

but not onto.

⟦ Because:

$$\nexists x\in\mathbb{N}\quad 2x=1\in\mathbb{N}.$$

⟧

এছাড়াও শত সহস্র counterexample সম্ভব, যেমন $f(x)=x+1$-এও দিব্যি কাজ চলত (এখানে $S=\mathbb{N}$). ■

এই প্রসঙ্গে শিব্রাম চক্রোত্তির একটা হাসির গল্প মনে পড়ল। পুরোটা মনে নেই, মূল ব্যাপারটা এইরকম--এক মঙ্গলবার শিব্রামের টাকার দরকার পড়েছে। তাই একশ টাকা ধার করেছে গোবর্ধনের কাছ থেকে। বলেছে যে, পরের মঙ্গলবার শোধ দিয়ে দেবে। এদিকে শিব্রাম টাকা তো বেমালুম খরচা করে ফেলেছে, পরের মঙ্গলে মাথায় হাত। তখন শিব্রাম দৌড়ে গেছে গোবর্ধনের দাদা হর্ষবর্ধনের কাছে। গিয়ে বলছে-- ভাই আমার এক্ষুণি একশ টাকা দরকার, তোমাকে পরের মঙ্গলবারে মিটিয়ে দেব। হর্ষবর্ধন ভালোমানুষ, দিয়ে দিয়েছে। শিব্রাম তখন সেই টাকা নিয়ে বুক ফুলিয়ে গোবর্ধনকে শোধ দিয়ে গেল। পরের মঙ্গলবারে হর্ষবর্ধনকে টাকা ফেরৎ দেবার পালা। অতএব শিব্রাম সটান গোবর্ধনের কাছে হাজির--আবার একশ টাকা চাই। শিব্রাম গত সপ্তাহে টাকা যথাসময়ে ফেরৎ দিতে একটুও কসুর করেনি, অতএব তাকে ফের টাকা ধার দিতে গোবর্ধনের কোনো আপত্তি নেই। এইভাবে বুঝতেই পারছ শিব্রামের দিব্যি চলছে, এক সপ্তাহে গোবর্ধনের ঘাড় ভেঙে হর্ষবর্ধনকে তুষ্ট রাখে, পরের সপ্তাহে উল্টোটা। সুতরাং সেই যে প্রথম একশ টাকা উড়িয়ে দিয়েছিল, তার কোনো খোঁজই পড়ে না। খালি প্রতি সপ্তাহে এর বাড়ি ওর বাড়ি দৌড়োদৌড়ি করতে হয় এই যা কষ্ট। শেষটা একদিন শিব্রাম দুইভাইকে এক সঙ্গে পেয়ে বলেই ফেলল--দ্যাখো গোব্রা, প্রতি এক সপ্তাহ অন্তর তুমি দাদাকে একশ টাকা দেবে, আর পরের সপ্তাহে সেটা দাদার থেকে ফেরৎ নিয়ে নেবে। কেমন, খুশী তো? আমাকে যেন বাপু সেই কবে একশ টাকা নিয়েছিলাম বলে গালমন্দ কোরো না!"
শিব্রাম বুদ্ধিটা চমৎকার ভেবেছিল, কিন্তু বাস্তবে এটা কাজ করবে না। কেন? কোনো না কোনো দিন তো জবাবদিহি করতেই হবে, যদি সবাই অমর হত তবে অসুবিধা ছিল না। একটা ছবি দেখলেই আমাদের আলোচনায় এই গল্পটার প্রাসঙ্গিকতা বুঝবে। Fig 59-এ আমরা শিব্রামের গোপন হিসেবের খাতাটা দেখিয়েছি। প্রতিটা তীর চিহ্ন মানে একটা করে ধার নেওয়া আর শোধের প্রতিশ্রুতি দেওয়া। যেমন, প্রথম মঙ্গলবার ধার নিয়ে দ্বিতীয় মঙ্গলবারের শোধ দেবার প্রতিশ্রুতি হল সবচেয়ে উপরের তীর চিহ্নটা। বুঝতেই পাচ্ছ যে সবগুলো তীর চিহ্ন মিলে আসলে একটা function হয় $f:\mathbb{N}\to\mathbb{N}$, যেখানে $f(n)=n+1$. এটা one-one, তাই দু ভাইয়ের কেউই কিছু সন্দেহ করছে না, কিন্তু onto নয়, তাই শিব্রাম টাকা মারতে পারছে। কিন্তু যদি কোনোদিন হিসেব মেটাতে হয়, মানে যদি infinite $\mathbb{N}$-এর বদলে কোনো finite set নিয়ে কাজ করি, তবে শেষের দিন গিয়ে সমস্যা হবে (Fig 60)।

Exercise 28: যদি S infinite হয় তবে এমন উদাহরণ দিতে পারো যেখানে f onto কিন্তু one-to-one নয়? ■

DAY 7
Function (part 4)

7.1 Composition

এবার আমরা function-এর composition নিয়ে আলোচনা করব। Composition মানে হল একটা function-এর পেটে আরেকটা function ঢুকিয়ে নতুন function বানানো। যেমন ধরো $f(x) = \sin x$ আর $g(x) = x^2$ নিলাম। যদি $g(x)$-কে $f(x)$-এর পেটে ঢুকিয়ে দিই তবে পাব $f(g(x)) = \sin x^2$. এটার একটা নতুন নাম দিই, ধরো, $h(x)$.

হাঁস ছিল, সজারুও, (ব্যাকরণ মানি না),
হয়ে গেল 'হাঁসজারু', কেমনে তা জানি না।
...
'হাতিমি'-র দশা দ্যাখো, তিমি ভাবে জলে যাই,
হাতি বলে এই বেলা জঙ্গলে চলো ভাই।

--সুকুমার রায়

তাহলে আমরা সংক্ষেপে লিখে থাকি $h = f \circ g$. আমরা চাইলে উল্টোটাও করতে পারতাম-- f-কে ঢোকাতে পারতাম g-এর পেটে তবে পেতাম $g(f(x)) = (\sin x)^2$. এটাকে সংক্ষেপে লিখব $g \circ f$. লক্ষ কর যে, এই উদাহরণে অন্ততঃ $g \circ f$ এবং $f \circ g$ আলাদা আলাদা function.

Function-এর composition যেন অনেকটা সুকুমার রায়ের আবোল তাবোলের মত--হাঁস আর সজারু মিলিয়ে হাঁসজারু তৈরী করা, কিংবা হাতির সাথে তিমি মিলিয়ে হাতিমি। কিন্তু যাকে খুশী যার তার সাথে মিলিয়ে দেওয়া যায় না। ব্যাকরণ মানেন নি বটে, কিন্তু স্বয়ং সুকুমার রায়ও সে কথা মাথায় রেখেছিলেন, হাঁসের পিছনে যে সজারুকে জোড়া গেছিল, তার কারণ 'হাঁস'-এর শেষে 'স' আছে আর 'সজারু'-র গোড়াতেও 'স' আছে। তেমনি 'হাতি' আর 'তিমি'-র যোগসূত্র রচনা করেছে ওই 'তি'-টা। একই যুক্তিতে 'রুই' আর 'ইলিশ' মিশিয়ে উপাদেয় রুইলিশ বানানো যেত, যদিও সুকুমার রায় সেটা করেন নি। Function-এর composition-এর বেলাতেও দেখে নিতে হয় ওরা সত্যিই 'ফিট্' করে কিনা। যেমন, যদি $f(x) = \log x$ হয় আর $g(x) = -x^2$ হয়, তবে তুমি $f(g(x)) = \log(-x^2)$ লিখতে পারো না, কারণ $-x^2 \leq 0$ এবং তাই তার log মোটেই defined নয়! অবশ্য $g(f(x)) = -(\log x)^2$ লিখতে কোনোই আপত্তি নেই। দুটো function 'ফিট্ করা' বলতে কী বোঝায়, সেটা নীচের সংজ্ঞায় দিলাম।

DEFINITION: Composition

Let $f : A_1 \to A_2$ and $g : B_1 \to B_2$ be two functions. If $A_2 \subseteq B_1$ then we can define the **composition** of f with g as the function $g \circ f : A_1 \to B_2$ as

$$(g \circ f)(x) = g(f(x)).$$

Similarly, if $B_2 \subseteq A_1$, then we can define $f \circ g : B_1 \to A_2$ as

$$(f \circ g)(x) = f(g(x)).$$

একটা অংক করে সংজ্ঞাটা সড়গড় হয়ে নেওয়া যাক।

Example 48: Let $f, g : \mathbb{R} \to \mathbb{R}$ be two functions given by $f(x) = |x| + x$ for all $x \in \mathbb{R}$, and $g(x) = |x| - x$ for all $x \in \mathbb{R}$. Find $f \circ g$.[3] **(2013)**

SOLUTION:

Here codomain of g is $\mathbb{R}$, which is the domain of f.
Hence $f \circ g$ is well defined.

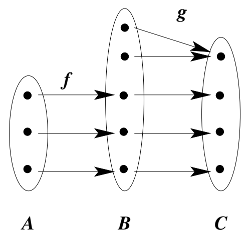


Fig 61

For $x \in \mathbb{R}$, we have

$$\begin{aligned}(f\circ g)(x) &= f(g(x))\\ &= |g(x)| + g(x)\\ &= \big||x|-x\big| + |x| - x\end{aligned}$$

এই বার লক্ষ কর যে, সবসময়েই $|x| \geq x$ হয়। তাই $|x| - x \geq 0$.
সুতরাং ওর absolute value নেওয়া আর না নেওয়া, একই ব্যাপার।

$$\begin{aligned}&= |x| - x + |x| - x \quad [\because |x| - x \geq 0]\\ &= 2(|x| - x).\end{aligned}$$

■

Example 49: State true or false with justification: $f : \mathbb{Z} \to \mathbb{Z}$, $g : \mathbb{Z} \to \mathbb{Z}$ are given by $f(x) = x + 1$ and $g(x) = 2x + 3$. Then $g \circ f$ is a surjective mapping.[2] **(2003)**
SOLUTION: প্রথম কাজ হল $g \circ f$ function-টার ফর্মুলাটা বার করা-- $(g\circ f)(x) = g(f(x)) = 2f(x) + 3 = 2(x + 1) + 3 = 2x + 5$.
এবার দেখতে হবে যে, এই $2x + 5$ function-টা $\mathbb{Z}$ থেকে $\mathbb{Z}$-এ surjective কিনা। খানিকক্ষণ নাড়াচাড়া করলেই চোখে পড়বে যে $2x + 5$ সবসময়েই একটা odd number অর্থাৎ বিজোড় সংখ্যা, কারণ $2x$ সর্বদাই জোড় মানে even, সুতরাং তার সাথে একটা বিজোড় সংখ্যা 5 যোগ করলে উত্তরটা odd হতে বাধ্য।
তার মানে $2x + 5$ কখনোই $\mathbb{Z}$-এর মধ্যেকার even value-গুলো নিতে পারবে না। ফলে surjective হওয়ার কোনো প্রশ্নই নেই। যথারীতি আমরা একটা counterexample দেব। যেকোনো একটা even number নাও, যেমন ধর 0, তবে $2x + 5 = 0$ হতে পারবে না, কারণ তার জন্য x-কে ভগ্নাংশ হতে হবে।

The statement is false.
Shall show that $g \circ f$ is not surjective, ie,

◎ $\exists y \in \mathbb{Z} \quad \forall x \in \mathbb{Z} \quad f(x) \neq y.$

$\exists y$ Choose $y = 0$.

$\forall x$ Take any $x \in \mathbb{Z}$.

Then

$$\begin{aligned}(g\circ f)(x) &= g(f(x))\\ &= 2f(x)+3\\ &= 2(x+1)+3\\ &= 2x+5,\end{aligned}$$

which is an odd number, and hence $\neq 0$, since 0 is an even number. So f is not surjective.

■

Composition করে দুটো function-কে জুড়ে দেওয়া যায় (যদি ফিট্ করে)। বার বার composition চালিয়ে গেলে দুয়ের বেশী function-কেও জোড়া যায়। যেমন $f(x)=\sin x$-এর পেটে $g(x)=x^2$ এবং তার পেটে $h(x)=\log x$ ভরে দিলে পাব

$$(f\circ g\circ h)(x)=\sin(\log x)^2.$$

সুকুমার রায় তো শুধু হাঁসের পিছনে সজারুকে জুড়েই ক্ষান্ত দিয়েছিলেন, তারপরে রুই মাছকে জুড়ে হাঁসজারুই বানানোর চেষ্টাটা করে দেখবে নাকি?

7.1.1 $f\circ g$ থেকে f আর g

দুটো জিনিস মিশিয়ে যখন একটা নতুন জিনিস তৈরী করা হয়, তখন নতুন জিনিসটার গুণাগুণ বিচার করে উপাদানগুলোর গুণাগুণ কিছুটা জানা যেতে পারে। এখানেও আমরা সেই চেষ্টা করব। $f\circ g$-এর কোনো বৈশিষ্ট্য দেওয়া থাকলে তা থেকে f বা g-এর সম্বন্ধে কিছু বলা যায় কি না দেখব।

Example 50: Let $f:A\to B$ and $g:B\to C$ be two mappings (A,B,C are nonempty sets).

Show that if $g\circ f$ is injective then f is injective, but g may not be so.[3] **(2010.2ci,2009.2ci)**

SOLUTION:

First part: To show $f:A\to B$ is injective, ie,

$$\forall a_1,a_2\in A\quad (f(a_1)=f(a_2)\implies a_1=a_2).$$

$\forall a_1,a_2$ Take any $a_1,a_2\in A$ with $f(a_1)=f(a_2)$. Then $g(f(a_1))=g(f(a_2))$,

ie, $(g\circ f)(a_1)=(g\circ f)(a_2)$.

Since $g\circ f$ is injective, hence $a_1=a_2$, as required.

এবার দ্বিতীয় অংশ--

Second part:

কেন g-এর injective হবার কোনো দরকার নেই সেটা Fig 61 থেকে বোঝা যাবে। এখানে দেখাই যাচ্ছে যে, g-টা injective নয়, কারণ ওপরের দুটো তীর চিহ্ন একই জায়গায় গিয়েছে। কিন্তু তাতে $g\circ f$-এর injective হবার কিছুমাত্র অসুবিধা হয় নি, কারণ f-এর তীর চিহ্নগুলো g-এর ওই ঝামেলাজনক অংশটাকে সম্পূর্ণ এড়িয়ে গিয়েছে। মনে রেখো অংকে কোনো কিছুকে ভুল প্রমাণ করতে চাইলে একখানা counterexample-ই যথেষ্ট। অতএব আলোচনার এখানেই ইতি টেনে এবার খালি ছবিটাকে algebra-র ভাষায় লেখার অপেক্ষা--

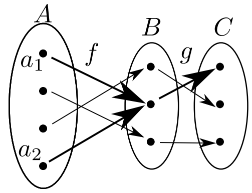


Fig 62

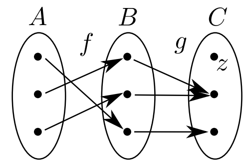


Fig 63

Counterexample:

Let $A = \{1,2,3\}$, $B = \{1,2,3,4,5\}$ and $C = \{1,2,3,4\}$.
Take $f : A \to B$ as $f(x) = x$.
Take $g : B \to C$ as

$$g(x) = \begin{cases} x & \text{if } x = 1,2,3,4 \\ 4 & \text{otherwise} \end{cases}$$

Then g is not injective, since $g(4) = g(5)$. But $(g \circ f)(x) = x$ for each $x \in A$.
So $g \circ f$ is injective.

■

Exercise 29: State true or false with justification: $f : A \to B$ and $g : B \to C$ are two mappings. If $g \circ f : A \to C$ is injective then g is injective.[2] **(2006)**

HINT:

The statement is false.

কেন সেটা তো আগের অংকের সমাধানের দ্বিতীয় অংশে লিখেইছি। ■

Exercise 30: Let $f : A \to B$ and $g : B \to C$ be two mappings such that $g \circ f$ is injective. Is it necessary that g is injective? Justify your answer.[2] **(2011.15ii)**

HINT:

আগের অংকটাই। ■

নীচের অংকটা এই ব্যাপারটাকেই আরেক ধাপ এগিয়ে নিয়ে গেছে। এখানে বাড়তি দিয়ে দিয়েছে যে, f-টা surjective. সুতরাং আমরা যে কায়দায় counterexample বানিয়েছিলাম (মানে f-এর তীরগুলোকে g-এর ঝামেলাজনক অংশটা এড়িয়ে নিয়েছিলাম), সেটা আর কাজ করবে না, কারণ surjective হওয়া মানে f-এর তীর সর্বত্রই পৌঁছতে হবে। এক্ষেত্রে g-এর injective হওয়া ছাড়া পথ নেই। সেটাই এবার দেখাব।

Example 51: Let $f : A \to B$ and $g : B \to C$ be two mappings such that $g \circ f$ is injective, and f is surjective. Prove that g is injective. [2] **(2014)**

SOLUTION:

To show

$\forall b_1, b_2 \in B \quad (g(b_1) = g(b_2) \implies b_1 = b_2).$

$\forall b_1, b_2$ Take any $b_1, b_2 \in B$ such that $g(b_1) = g(b_2)$.

$\because f : A \to B$ is surjective,

$\therefore b_1 = f(a_1)$ and $b_2 = f(a_2)$ for some $a_1, a_2 \in A$.

So $g(f(a_1)) = g(f(a_2))$, or $(g \circ f)(a_1) = (g \circ f)(a_2)$.

Since $g \circ f$ is injective, this implies $a_1 = a_2$.

So $g(a_1) = g(a_2)$, or $b_1 = b_2$, as required.

■

Example 52: Let $f : A \to B$ and $g : B \to C$ be two mappings. If $g \circ f : A \to C$ is bijective, prove that f is injective and g is surjective.[5] **(2002)**

SOLUTION: দেওয়া আছে যে, $g \circ f$ bijective, অর্থাৎ একইসঙ্গে injective এবং surjective. দেখাতে হবে যে, f-টা injective হতে বাধ্য এবং g-টা surjective হতে বাধ্য। ঠিক যেন $g \circ f$ তার দুটো বৈশিষ্ট্যকে f আর g-র মধ্যে ভাগ করে দিয়েছে, তাতে f-এর ভাগে পড়েছে injective আর g-এর ভাগে পড়েছে surjective.

প্রথমে দেখি f-কে কেন injective হতেই হবে। যদি f-টা injective না হত তবে কী হত তার একটা উদাহরণ Fig 62-এ দেখানো হল। এখানে f injective নয়, কারণ $f(a_1) = f(a_2)$. অতএব a_1 বা a_2 যেখান থেকেই শুরু করি না কেন আমরা f-এর তীরচিহ্ন ধরে একই জায়গায় পৌঁছব। অর্থাৎ একবার f লাগাবার পর a_1 এবং a_2 থেকে বেরোনো তীর দুটো একসাথে জুড়ে গিয়েছে। এর পর g যাই হোক না কেন ওরা আর আলাদা হতে পারবে না, ফলে $g(f(a_1)) = g(f(a_2))$ হবে। তার মানে $g \circ f$ আর injective থাকবে না।

Let, if possible, $f : A \to B$ be not injective, ie,

$$\exists a_1, a_2 \in A \quad \big(a_1 \neq a_2 \text{ but } f(a_1) = f(a_2)\big).$$

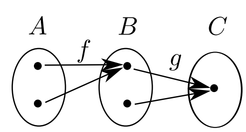
Then $(g \circ f)(a_1) = g(f(a_1)) = g(f(a_2)) = (g \circ f)(a_2)$.

$\because a_1 \neq a_2$, $\therefore$ this means $g \circ f$ is not injective ($\Rightarrow\Leftarrow$).

So f must be injective.

ওই "$\Rightarrow\Leftarrow$" চিহ্নটা মানে যে contradiction (অর্থাৎ এমন কিছু যেটা হতে পারে না) সেটা তো আগেই বলেছি। এখানে দেওয়া ছিল যে $g \circ f$ bijective, কিন্তু আমরা এদিকে সিদ্ধান্ত করে বসে আছি যে $g \circ f$ injective পর্যন্ত নয়! দুটো তো আর একসঙ্গে চলতে পারে না! সেই কারণেই এই contradiction. কিন্তু খামোখা এই গোলমালটা বাঁধিয়ে আমাদের লাভ কি হল? আমাদের দেখাতে বলেছিল যে f-টা injective হবে। আমরা তার উল্টোটা ধরে শুরু করেছিলাম-- "Let, if

Fig 64



possible, f be not injective." সেখান থেকে এসে উপস্থিত হলাম একটা contradiction-এ। তার মানে f-এর পক্ষে injective না হওয়া অসম্ভব, অর্থাৎ f-টা injective হতে বাধ্য! এইরকম ঘুরিয়ে নাক দেখানো প্রমাণকে বলে "proof by contradiction", যার উল্লেখ আমরা আগেই করেছি।
এবার দেখাব যে, g surjective হতে বাধ্য। প্রথমে ভেবে নিই যে, g যদি surjective না হত তবে কোথায় ঝামেলাটা বাঁধত। Fig 63 দ্যাখো।
এই ছবিতে দেখাই যাচ্ছে যে g surjective নয়, কারণ ওপরের ওই z বিন্দুটাতে কোনো তীরচিহ্ন পৌঁছয় নি। কিন্তু g যদি z-এ পৌঁছতে না পারে, তবে $g \circ f$-ই বা পারবে কি করে? কারণ B থেকে C-তে নিয়ে যাবার সম্পূর্ণ দ্বায়িত্ব তো g-এর। সেখানে g যদি বেঁকে বসে z-এ যাব না বলে, তবে খালি f দিয়ে হাজার চেষ্টা করেও $g \circ f$-কে surjective বানানো যাবে না!
আমরা যেভাবে চিন্তা করলাম সেটা হল by contradiction. প্রথমে g surjective নয় ধরে সিদ্ধান্ত করলাম যে $g \circ f$-ও surjective হতে পারে না। ইচ্ছে করলে আমরা contradiction-এর মধ্যে না গিয়েও প্রমাণটা করতে পারি। প্রথমে লিখে নিই কী দেখাতে হবে--

> To show that $g : B \to C$ is surjective, ie,
>
> $\forall c \in C \quad \exists b \in B \quad g(b) = c.$

যেকোনো একটা c ধরে নিয়ে শুরু করি।

> $\forall c$ Take any $c \in C$.

যেহেতু $g \circ f$ হল surjective তাই $g \circ f$-এর তীর কোনোভাবে c-তে পৌঁছতে পারে--

> Since $g \circ f : A \to C$ is surjective, so $(g \circ f)(a) = c$ for some $a \in A$.
>
> Thus, $g(f(a)) = c$.
>
> $\exists b$ Choose $b = f(a) \in B$.
>
> Then $g(b) = g(f(a)) = c$, as required.

■

Example 53: If $f : A \to B$ and $g : B \to C$ are two mappings such that $g \circ f : A \to C$ is surjective, is it necessary for f to be surjective? Justify your answer.[2] **(2013)**
SOLUTION: এই অংকটা ছবি দিয়ে ভাবলে সুবিধা হবে। Fig 64 দেখলেই বুঝবে যে, f-টা surjective নাও হতে পারে।

> No, f need not be surjective. For example, we can take $A = \{1, 2\}$, $B = \{1, 2\}$ and $C = \{1\}$. We define $f : A \to B$ as $f(1) = f(2) = 1$, and $g : B \to C$ as $g(1) = g(2) = 1$.
>
> Then $g \circ f : A \to C$ is $(g \circ f)(1) = g(f(1)) = g(1) = 1$ and $(g \circ f)(2) = g(f(2)) = g(1) = 1$.
>
> So $g \circ f$ is surjective, but f is not surjective, since $\nexists a \in A \quad f(a) = 2$.

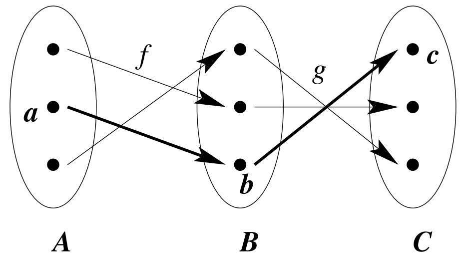


Fig 65

■

Exercise 31: Give an example to show that f need not be surjective if $g \circ f$ is surjective. **(2008)**
HINT: আগের অংকটারই রকমফের। ■

কিন্তু যদি একটা বাড়তি শর্ত দিয়ে দিই যে, g-টা injective, তবে কিন্তু f-কে surjective হতে হবে। সেটাই নীচের অংকটার বক্তব্য।

Example 54: Let $f : A \to B$ and $g : B \to C$ be two mappings. Prove that f is surjective if $g \circ f$ is surjective and g is injective.[2] **(2012.15ii)**
SOLUTION:

To show: $f : A \to B$ is surjective, ie,

$\forall b \in B \quad \exists a \in A \quad f(a) = b.$

$\forall b$ Take any $b \in B$.

Let $c = g(b) \in C$.

$\because g \circ f : A \to C$ is surjective,

$\therefore \exists a \in A \;\; g(f(a)) = c.$

$\exists a$ Choose this $a \in A$.

We have $g(f(a)) = c = g(b)$.

But g is injective.

So $f(a) = b$, as required.

■

7.1.2 f আর g থেকে $f \circ g$

Example 55: If $f : A \to B$ and $g : B \to C$ are two bijective mappings, prove that $g \circ f : A \to C$

is also bijective. $[g \circ f(a) = g\{f(a)\}.][2]$ **(2005)**

SOLUTION: দেখাতে হবে যে দুটো bijective মিলে bijective-ই হয়। কোনো function-কে bijective দেখানো মানে তাকে injective এবং surjective দেখানো। সাধারণতঃ এইদুটো জিনিস আলাদা আলাদা ধাপে দেখাতে হয়।

> Shall show that $g \circ f : A \to C$ is bijective,
> ie, it is injective and surjective.

Injective আর surjective-এর মধ্যে কাকে আগে দেখাব, তাতে কিছুই এসে যায় না। আমরা এখানে প্রথম ধাপে injective দেখাব। Injective দেখানোর মূল কায়দা একটাই-- domain-এর মধ্যে দুটো element নিয়ে শুরু কর যাদের ক্ষেত্রে function-টার value সমান। তারপর কোনোভাবে দেখাও যে, তাহলে দুটো element আসলে একই element হতে বাধ্য।

> Step 1: Shall show $g \circ f$ is injective, ie,
> $\forall a_1, a_2 \in A \quad \big((g \circ f)(a_1) = (g \circ f)(a_2) \implies a_1 = a_2\big).$
> $\boxed{\forall a_1, a_2}$ Take any $a_1, a_2 \in A$ with $(g \circ f)(a_1) = (g \circ f)(a_2)$.

বলা আছে যে g হল injective. সুতরাং--

> $\because g : B \to C$ is injective, and $g(f(a_1)) = g(f(a_2))$,
> $\therefore f(a_1) = f(a_2)$.

আবার f-ও তো একটা injective function. তাই--

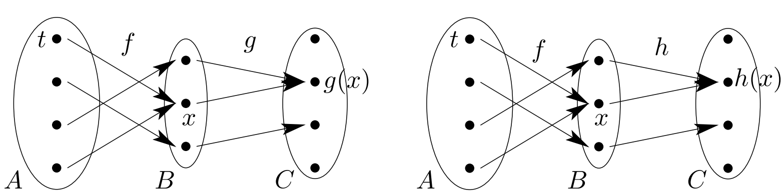
> $\because f : A \to B$ is also injective,
> $\therefore a_1 = a_2$, as required.

পরের ধাপে surjective দেখাব। তার জন্য Fig 65-টা মাথায় রাখো।

> Step 2: Shall show that $g \circ f$ is surjective, ie,
> $\forall c \in C \quad \exists a \in A \quad (g \circ f)(a) = c.$
> $\boxed{\forall c}$ Take any $c \in C$.

যেহেতু g surjective তাই g-এর কোনো না কোনো তীর c-তে গিয়েছে। এই তীরের গোড়াটা আছে B-এর মধ্যে কোথাও, ধরো b-তে।

Fig 66



(a) (b)

$\because g : B \to C$ is surjective,

$\therefore \exists b \in B \quad g(b) = c.$

এদিকে f-ও surjective, সুতরাং f-এর কোনো একটা তীর এসে b-এর কূলে ভিড়েছে, সেই তীরটা ধরে উল্টোদিকে চললে পৌঁছব A-র কোনো একটা element-এ। ধরি তার নাম a.

Again, $\because f : A \to B$ is surjective,

$\therefore \exists a \in A \quad f(a) = b.$

$\exists a$ Choose this $a \in A$.

তার মানে a থেকে প্রথমে f এবং তারপরে g লাগিয়ে c-তে যাওয়া যায়।

Then $(g \circ f)(a) = g(f(a)) = g(b) = c$, as required.

■

Exercise 32: If $f : A \to B$ and $g : B \to C$ are both surjective, then prove that the composite mapping $g \circ f : A \to C$ is surjective. **(2008)**
HINT: আগের অংকের সমাধানের দ্বিতীয় ধাপটুকু করে দিলেই হবে। ■

Example 56: Let $f : A \to B$, $g : B \to C$ and $h : B \to C$ be three mappings such that f is surjective and $g \circ f = h \circ f$. Prove that $g = h$.[3] **(1999)**
SOLUTION: এখানে আমাদের কাজ হচ্ছে দুটো function-কে সমান দেখানো।

To show $g = h$,

প্রথমে বোঝা যাক দুটো function কী হলে সমান হয়। একটা function-এর তিনটে অঙ্গ থাকে, যেমন $p : [0, 2] \to [0, 4]$ যদি হয় $p(x) = x^2$ তবে তার অঙ্গ তিনটে হল domain $[0, 2]$, codomain $[0, 4]$ এবং তার ফর্মুলা $p(x) = x^2$. দুটো function-কে সমান দেখানো মানে এইটা দেখানো যে ওদের তিনটে অঙ্গই অভিন্ন, অর্থাৎ ওদের দুজনেরই একই domain, একই codomain এবং একই ফর্মুলা।
এই অংকে অবশ্য g এবং h দুজনেরই domain দেওয়াই আছে এক--B. আবার codomain-ও দেওয়া আছে এক--C. সুতরাং খালি ফর্মুলাদুটো এক দেখাতে পারলেই হবে।

Fig 67

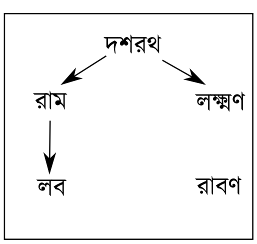


Fig 68

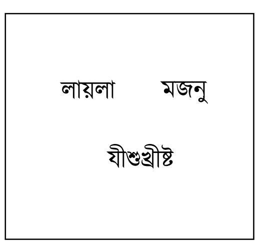


Fig 69

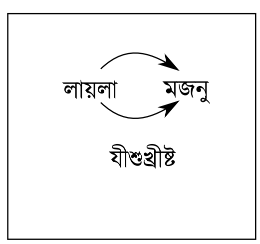
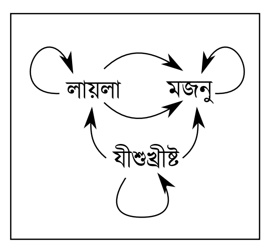


Fig 70



ie, to show that

1. g and h have the same domain ($= B$, given)
2. g and h have the same codomain ($= C$, given)
3. $\forall x \in B \quad g(x) = h(x)$.

আমাদের খালি তিন নম্বরটা দেখালেই চলবে।

Take any $x \in B$.

দেখাতে চাই যে, $g(x) = h(x)$. কিন্তু $g(x)$ বা $h(x)$ কারোরই ফর্মুলা সরাসরি দেওয়া নেই। খালি বলা আছে যে $g \circ f = h \circ f$. সুতরাং কোনোভাবে আমাদেরকে g থেকে $g \circ f$-এ এবং h থেকে $h \circ f$-এ গিয়ে পড়তে হবে। তাহলেই কেল্লা ফতে! Fig 66 দ্যাখো।

$\because f : A \to B$ is surjective,

$\therefore x = f(t)$ for some $t \in A$.

So

$$\begin{aligned} g(x) &= g(f(t)) = (g \circ f)(t) \\ &= (h \circ f)(t) \quad [\because g \circ f = h \circ f.] \\ &= h(f(t)) = h(x), \end{aligned}$$

as required.

■

DAY 8
Relation (part 1)

এবার আমরা relation বলে আরেকটা জিনিস শিখব, যেটাও function-এর মত তীর চিহ্ন এঁকে বোঝা যায়। একটা উদাহরণ নিয়ে শুরু করি। Relation মানে হল সম্পর্ক, একটা সম্পর্কের উদাহরণ নিই, ধরো বাবা-ছেলে সম্পর্ক। Fig 67-এ রামায়ণের কিছু চরিত্রের set রয়েছে। আমরা এদের মধ্যে বাবা-ছেলে সম্পর্ক বুঝিয়েছি বাবার থেকে ছেলেতে তীর চিহ্ন এঁকে।
আরেকটা উদাহরণ নিই, এবার set-টা হল Fig 68-এর মত। Relation-টা হল কে কাকে ভালোবাসে। তুমি হয় তো ভাবছ তীর চিহ্নগুলো হবে খালি Fig 69-র মত। কিন্তু ভুলে যেও না, যীশুখ্রীষ্ট আবার সকলকেই ভালোবাসেন। আর সত্যি বলতে কি, নিজেকে তো সকলেই ভালোবাসে, তাই না? সুতরাং এখানে relation-টার ছবি হবে Fig 70-এর মত।
এরকমভাবে তীর চিহ্ন দিয়ে না বুঝিয়ে অবশ্য আমরা সরাসরি কে কাকে ভালোবাসে তার একটা লম্বা তালিকা করে দিতে পারতাম--

লায়লা ভালোবাসে মজনুকে
মজনু ভালোবাসে লায়লাকে,
ইত্যাদি।

এইভাবে লিখতে লিখতে হাত ব্যথা হয়ে যাবার সম্ভাবনা, তাই এত কিছু না লিখে অনেক সময়ে SMS লেখার মত সংক্ষেপে লিখি--

লায়লা $\heartsuit$ মজনু, ইত্যাদি।

এখানে $\heartsuit$ হল আমাদের relation-টার চিহ্ন। সব সময়ে অবশ্য এমন তৈরী চিহ্ন পাওয়া যায় না। তখন আমরা যা হোক একটা অক্ষর দিয়ে কাজ চালাই। যেমন যদি বাবা-ছেলে সম্পর্কটার জন্য R চিহ্নটা ব্যবহার করি, তবে "দশরথ রামের বাবা" এই কথাটাকে সংক্ষেপে লিখতে পারি "দশরথ R রাম"। এরকম লেখা দেখে হয়তো হাসি পেতে পারে, কিন্তু এই কায়দাটা আমাদের খুব অচেনা কিছু কিন্তু নয়। যেমন "কে কার থেকে বড়" সেটা একটা relation, এর জন্য চিহ্ন হল $>$. তাই আমরা "5 সংখ্যাটা 3-এর চেয়ে বড়" এই কথাটাকে সংক্ষেপে লিখে থাকি $5 > 3$. অনেক সময়ে আমরা অবশ্য আলাদা কোনো চিহ্নই ব্যবহার করি না। সরাসরি একটার পর একটা কমা দিয়ে লিখে দিই। যেমন "কে কার বাবা" সেটা বোঝাতে পারি এইভাবে--

{(দশরথ, রাম), (দশরথ, লক্ষ্মণ), (রাম, লব)}.

এখানে প্রত্যেকটা বাবা-ছেলে জুটিকে আমরা ফার্স্ট ব্র্যাকেট (যাকে ইংরাজীতে বলে parentheses)-এর মধ্যে লিখেছি। প্রতি ক্ষেত্রে একই ক্রম বজায় রেখেছি--আগে বাবা, পরে ছেলে। মাঝখানে একটা কমা বসিয়েছি।
লক্ষ কর এইভাবে লেখার ফলে আমরা একটা relation-কে একটা set বলে ভাবতে পারছি, যেটা আমাদের অতি পরিচিত জিনিস। এই set-এর প্রত্যেকটা element হল একজোড়া নাম দিয়ে তৈরী। সুতরাং নামগুলোর set-টাকে যদি A বলি, তবে relation-টা আসলে $A \times A$-র একটা subset ছাড়া কিছুই নয়! অংকের জগতে এইটাকেই relation-এর সংজ্ঞা বলে ধরা হয়--

DEFINITION: (Binary) relation

Let A be any nonempty set. By a **(binary) relation** on A we mean any subset (possibly empty) of $A \times A$.

আমরা যে ধরণের relation আলোচনা করছি, সেখানে relation-টা দুজনের মধ্যে হচ্ছে, সেই কারণে এই ধরণের relation-কে অনেক সময়ে binary relation বলে। তবে মনে রেখো যে, এই "দুজন" কিন্তু আলাদা আলাদা নাও হতে পারে। যেমন, ভালোবাসার উদাহরণে সকলেই নিজেকে ভালো ভালোবাসে, সুতরাং লায়লাও লায়লাকে ভালোবাসে, মানে "লায়লা $\heartsuit$ লায়লা", এখানে লায়লা একাই "দুজন"-এর ভূমিকা পালন করছে।
একটা relation হল একটা set, এবং সংজ্ঞাতে বলা হয়েছে যে, সেটা empty হলেও আপত্তি নেই। একটা empty relation-এর উদাহরণ দেখা যাক।

Example 57: যদি $A =$ {বুদ্ধদেব, হিটলার, চ্যাপলিন} নিই, তবে "কে কার বাবা" relation-টা যে empty relation হবে সেটা কি আর বলে দিতে হবে? ■

Relation-দের বিভিন্নভাবে শ্রেণীবিভাগ করা যায়। একধরণের relation আছে যারা দুমুখো। যদি a-র সঙ্গে b-এর সম্পর্ক থাকে, তবে b-এর সঙ্গেও a-র একই সম্পর্ক থাকবে। একটা উদাহরণ হল "সমবয়সী হওয়া"। আমি যদি তোমার সমবয়সী হই, তবে তুমিও আমার সমবয়সী হতে বাধ্য। কিন্তু "ভাই" সম্পর্কটার ক্ষেত্রে এটা কিন্তু খাটে না। অশোক অনিন্দিতার ভাই, কিন্তু তা বলে অনিন্দিতাকে নিশ্চয়ই অশোকের ভাই বলা যায় না! কিন্তু যদি আমরা সম্পর্কটাকে কেবল ছেলেদের মধ্যে সীমাবদ্ধ রাখি, তবে "ভাই"-ও একটা দুমুখো সম্পর্ক। আমরা যাকে দুমুখো সম্পর্ক বলছি, অংকের ভদ্রভাষায় তাকে বলে symmetric relation. এর সংজ্ঞাটা এইরকম--

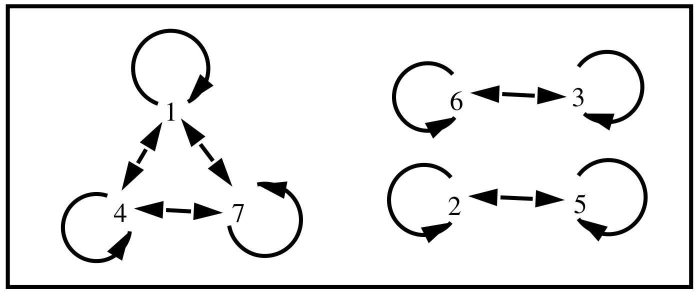


Fig 71

DEFINITION: **Symmetric relation**

A relation R on a nonempty set A is called **symmetric** if

$$\forall a, b \in A \quad \big(aRb \implies bRa\big).$$

আরেক রকম relation হয় তাদের বলে reflexive. এরকম relation-এর বেলায় সবাই নিজের সঙ্গে সম্পর্কিত হয়, যেমন সেই লায়লা-মজনু-যীশুখ্রীষ্টর উদাহরণে আমরা বলেছিলাম যে, সকলেই নিজেকে ভালোবাসে। সংজ্ঞাটা এরকম--

DEFINITION: **Reflexive relation**

A relation R on a nonempty set A is called **reflexive** if

$$\forall a \in A \quad aRa.$$

এবার আরেক ধরণের relation-এর কথা শিখব, তাকে বলে transitive. তার জন্য আগে একটা প্রশ্নের উত্তর দাও--তোমার বন্ধুর সব বন্ধুরাই কি তোমারও বন্ধু? উত্তর অবশ্যই 'না'। যেমন, সৈকত কলকাতায় যে মেসে থাকে সেই মেসে রামিজও থাকে, সেই সূত্রে রামিজ সৈকতের বেজায় বন্ধু। রামিজের বাড়ি মালদায়, সেখানে রামিজের ছোটোবেলার বন্ধু করিম, তাকে সৈকত চেনেও না! কিন্তু অনেক relation-এর ক্ষেত্রে ব্যাপারটা অন্য রকম। যেমন যদি $\mathbb{Z}$-এর উপরে '$>$' relation-টা নিই, তবে $a > b$ এবং $b > c$ হলে তৎক্ষণাৎ বলা যাবে যে $a > c$. এই ধরণের relation-কেই বলে transitive. "কে কার বন্ধু" এই relation-টা আমাদের সৈকত-রামিজ-করিমের উদাহরণে transitive ছিল না।

DEFINITION: **Transitive relation**

A relation R on a nonempty set A is called **transitive** if

$$\forall a, b, c \in A \quad \big([aRb \ \& \ bRc] \implies aRc\big).$$

Example 58: State true or false with justification: On the set $\mathbb{Z}$ of all integers a relation ρ is defined by $a\rho b$ if $ab \geq 0$. Then ρ is reflexive and transitive.[2] **(2004)**

SOLUTION:

> ρ is reflexive:
>
> $\forall a \in \mathbb{Z}$ we have $aa = a^2 \geq 0$. So $a\rho a$.
>
> ρ is not transitive:
>
> For example, $1\rho 0$ and $0\rho(-1)$,
>
> ⟦ Because:
>
> $1 \times 0 = 0 \geq 0$ and $0 \times (-1) = 0 \geq 0$.
>
> ⟧
>
> but $1 \not\rho (-1)$, since $1 \times (-1) = -1 \not\geq 0$.

■

8.1 Equivalence relation

অংকের জগতে এক ধরণের relation বার বার কাজে লাগে। এই relation-গুলোর মূল কথাটা হল--aRb হবে যদি a আর b-এর কোনো একটা বৈশিষ্ট্য এক হয়। এরকম একটা relation-এর উল্লেখ আগেই করেছি--সমবয়সী হওয়া। এখানে বৈশিষ্ট্যটা হল "বয়স"। যদি a আর b-র বয়স এক হয় তবেই বলব aRb. কিংবা বৈশিষ্ট্যটা হতে পারত "ধর্মবিশ্বাস"। সে ক্ষেত্রে a, b যদি দুজনেরই ধর্মবিশ্বাস এক হয় (দুজনেই হিন্দু, বা দুজনেই মুসলিম, বা দুজনেই নাস্তিক, ইত্যাদি) তবেই বলব aRb. আরেকটা উদাহরণ এরকম--ধরো set-টা নিলাম $A = \{1, 2, 3, 4, 5, 6, 7\}$, আর বৈশিষ্ট্যটা নিলাম "3 দিয়ে ভাগ করলে কত ভাগশেষ থাকে" সেটা। তার মানে যদি $a, b \in A$ হয় তবে aRb বলব একমাত্র তখনই যদি 3 দিয়ে ভাগ করলে দুজনেই সমান ভাগশেষ দেয়। যেমন $4R7$ কিন্তু $1\not R5$. এই রকম relation-এর ক্ষেত্রে যদি তীর চিহ্ন দিয়ে ছবি আঁকতে যাও, তবে একটা প্যাটার্ণ লক্ষ করবে (Fig 71)। এখানে set-এর element-গুলো দলে দলে জটলা পাকিয়ে আছে। একটা দলে আছে $1, 4, 7$. এদের সবার ক্ষেত্রেই ভাগশেষ হল 1. তাই এরা নিজেদের মধ্যে সবাই সবার সঙ্গে সম্পর্কিত। যাদের ক্ষেত্রে ভাগশেষ 2, তারা আবার নিজেদের মধ্যে আরেকটা দল বেঁধেছে-- $2, 5$. এরাও নিজেদের মধ্যে সবাই সবার সঙ্গে সম্পর্কিত। তৃতীয় দলে আছে যাদের বেলায় ভাগশেষ 0. এরাও নিজেদের মধ্যে সবাই সবার সঙ্গে সম্পর্কিত। এরকম relation-কে বলে equivalence.

ধর্মবিশ্বাসের উদাহরণেও একই ব্যাপার--যাবতীয় হিন্দুরা একটা দলে থাকবে, যাবতীয় মুসলিমরা আরেকটা দলে, ইত্যাদি। যখনই এরকম দলাদলি দেখবে, অমনি জানবে এর পিছনে একটা equivalence relation লুকিয়ে আছে।

একটু চিন্তা করলেই বুঝবে যে, এরকম দলাদলির relation সবসময়ে reflexive হতে বাধ্য--আমার দলে আর কেউ না থাক, আমি তো থাকবই! আবার আমার দলে যদি তুমি থাকো, তাহলে তোমার দলে আমিও আছি (কারণ আমার দল আর তোমার দল তো আসলে একই দল--আমাদের দল)। সুতরাং relation-টা symmetric হতেও বাধ্য। আবার তুমি আর আমি যদি একই ধর্মাবলম্বী হই, এবং তুমি আর তোমার প্রতিবেশী যদি এক ধর্মাবলম্বী হও, তবে আমার ধর্ম আর তোমার প্রতিবেশীর ধর্মও এক হবে। সুতরাং relation-টা transitive-ও বটে!

মজার কথা হল, এক্ষুণি যা বললাম তার উল্টোটাও ঠিক--যদি একটা relation একইসঙ্গে reflexive, symmetric এবং transitive হয়, তবে তার তীর চিহ্নগুলো আঁকলে দেখবে পুরো set-টা দলে দলে ভেঙে গেছে। প্রতিটা দলের মধ্যে সবাই সবার সঙ্গে সম্পর্কিত, কিন্তু দুটো আলাদা দলের সদস্যদের মধ্যে মুখ দেখাদেখি নেই! এই থেকেই নীচের সংজ্ঞাটার জন্ম--

Example 59: Define 'equivalence relation' on a nonempty set S.[1] **(2001,2004,2006)**

SOLUTION: এই সংজ্ঞাটা অংকের দুনিয়ার অত্যন্ত গুরুত্বপূর্ণ সংজ্ঞাগুলোর অন্যতম। খুব ভালো করে মনে রেখো।

DEFINITION: Equivalence relation

Let S be a nonempty set. A binary relation R is called an equivalence relation if

1. R is reflexive, ie,
$$\forall x \in S \quad xRx.$$
2. R is symmetric, ie,
$$\forall x, y \in S \quad (xRy \implies yRx).$$
3. R is transitive, ie,
$$\forall x, y, z \in S \quad ([xRy \quad \& \quad yRz] \implies xRz).$$

এই definition-এ দুটো জিনিস লক্ষ করো-- এক, S-কে nonempty হতে হবে। দুই, আমরা এখানে ব্যবহৃত প্রত্যেকটা term-কেই অংকের ভাষায় লিখেছি, যেমন খালি reflexive, symmetric আর transitive এই তিনটে কথা লিখেই ছেড়ে দিই নি, তাদের অর্থ $\forall$-ইত্যাদি দিয়ে বুঝিয়ে লিখেছি। ■

Exercise 33: Define equivalence relation on a set S.[1] **(1998)**
HINT:
আগের অংকটাই। এখানে nonempty না বলে দিলেও সেটা ধরে নিতে হবে। ■

8.2 পরীক্ষা করে দেখা

এবার কিছু অংক করব, যেখানে একটা relation দেওয়া থাকবে, আর আমাদের পরীক্ষা করে দেখতে হবে সেটা একটা equivalence কিনা।

Example 60: In each case examine whether the relation ρ is an equivalence relation on the set S of all integers.

1. $\rho = \{(a, b) \in S \times S : |a - b| \leq 3\}$,
2. $\rho = \{(a, b) \in S \times S : a - b \text{ is a multiple of } 6\}$.

(1997)
SOLUTION:

1. যখন কোনো একটা relation দিয়ে জানতে চাওয়া হয় যে, সেটা একটা equivalence কিনা, তখন মনে মনে একবার চট্‌ করে দেখে নেওয়া ভালো যে reflexive, symmetric আর transitive এই তিনটে শর্তই পালিত হয়েছে কিনা। যদি অন্ততঃ একটাও না হয়, তবে সেটা লিখে বলে দিলেই চলবে যে relation-টা একটা equivalence নয়। যদি তিনটেই পালিত হয়, তবে অবশ্য তিনটেকেই প্রমাণ করতে হবে।

   আমাদের relation-টা হচ্ছে ρ, যেখানে $(a, b) \in \rho$ মানে $|a - b| \leq 3$, তার মানে a আর b-র দূরত্ব 3-এর কম।

- Reflexive? a-র থেকে a-র দূরত্ব 0, সেটা ≤ 3, সুতরাং reflexive.
- Symmetric? a-র থেকে b যত দূরে, b থেকে a-ও ঠিক ততটাই দূরে, তাই symmetric.
- Transitive? মানে a-র 3 মাইলের মধ্যে b, আর b-র 3 মাইলের মধ্যে c থাকলে c আর a-র দূরত্ব কি 3 মাইলের কম হতে বাধ্য? মোটেই না, কারণ a আর c এরা দুজনে b-এর দুই বিপরীত দিকে থাকতে পারে।

> No, the relation is not an equivalence, because it is not transitive.

কিন্তু এটুকু লেখাই যথেষ্ট নয়, ভুল প্রমাণ করতে হলে counterexample চাই। কী করে বানাবো সেটা তো জেনেই গিয়েছি-- a আর c-কে b-এর দুই বিপরীত দিকে নিতে হবে, যেমন $b = 3$ নিলে, $a = 1$ আর $c = 5$ নিতে পারি।

> For example, $(1, 3) \in \rho$ and $(3, 5) \in \rho$ but $(1, 5) \notin \rho$.

2. এখানেও প্রথমে মনে মনে দেখে নিয়েছি যে তিনটে শর্তই পালিত হয় কিনা। এখানে হয়েছে। তাই--

> Yes, the relation is an equivalence.

এবার তিনটে শর্তকে আলাদা আলাদা করে প্রমাণ করব। প্রতি ক্ষেত্রে প্রথমে লিখে নেব শর্তটা কী, তারপর সেটাকে প্রমাণ করব।

> <u>Reflexivity:</u> To show
>
> $\forall a \in S \quad (a, a) \in \rho.$
>
> [$\forall a$] Take any $a \in S$.
>
> Then $(a - a) = 0 = 0 \times 6$, which is a multiple of 6.
> $\therefore (a, a) \in \rho$, as required.
>
> <u>Symmetry:</u> To show
>
> $\forall a, b \in S \quad \big((a, b) \in \rho \implies (b, a) \in \rho\big).$
>
> [$\forall a, b$] Take any $a, b \in S$ with $(a, b) \in \rho$.
>
> Then $a - b = 6n$ for some integer n.
> $\therefore b - a = -6n$ is a multiple of 6.
> $\therefore (b, a) \in \rho$, as required.
>
> <u>Transitivity:</u> To show
>
> $\forall a, b, c \in S \quad \big([(a, b) \in \rho \,\&\, (b, c) \in \rho] \implies (a, c) \in \rho\big).$
>
> [$\forall a, b, c$] Take any $a, b, c \in S$ with $(a, b) \in \rho$ and $(b, c) \in \rho$.
>
> Then $a - b = 6n$ for some integer n, and $b - c = 6m$ for some integer m.
> $\therefore a - c = (a - b) + (b - c) = 6(n + m)$ is a multiple of 6.
> $\therefore (a, c) \in \rho$, as required.

■

Example 61: A relation ρ on the set of integers $\mathbb{Z}$ is defined by

$$\rho = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} : |a - b| \leq 5\}.$$

Is the relation reflexive, symmetric and transitive?[3] **(2003)**
SOLUTION: আগের অংকের প্রথম অংশের মত। তাই আর বিস্তারিত বর্ণনায় যাচ্ছি না। ■

Example 62: Which of the following relations is an equivalence relation on the set of integers $\mathbb{Z}$?

1. $P = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid xy \geq x\}$,
2. $Q = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid x - y \text{ is a multiple of } 5\}$.

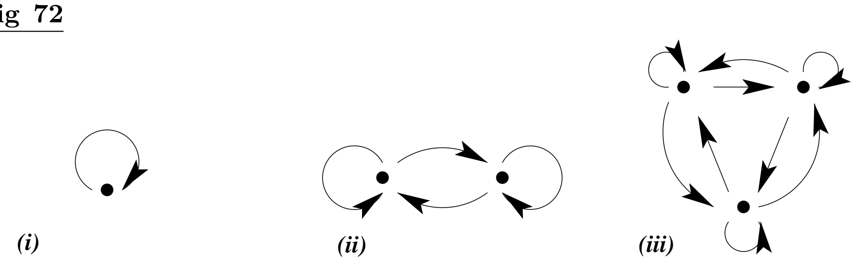
Give reasons in support of your answer.[3] **(1998)**
SOLUTION:

1. কোনো relation-কে যদি পরীক্ষা করে দেখতে হয় সেটা equivalence কি না, তার জন্য মনে মনে তিনটে শর্তকে পরীক্ষা করে দেখতে হয়। কোনটা দিয়ে শুরু করব? যেটা দিয়ে খুশী করা যায়, কিন্তু লক্ষ কর যে relation-টা হল $xy \geq x$. এর মধ্যে x আর y দুজনে একটু আলাদাভাবে উপস্থিত, ডানদিকে খালি x রয়েছে, y নেই। এটা দেখে স্বভাবতঃই সন্দেহ জাগে এই relation-এর symmetry সম্বন্ধে। সুতরাং সেটাকেই প্রথমে পরীক্ষা করি। যদি $x = -1, y = 1$ নিই তবেই দেখা যাচ্ছে যে symmetric হচ্ছে না।

   > P is not an equivalence, because it is not symmetric. For example,
   >
   > $$(-1, 1) \in P \text{ since } -1 \times 1 \geq -1,$$
   >
   > but
   >
   > $$(1, -1) \notin P \text{ since } 1 \times (-1) \not\geq 1$$

2. পরের relation-টা নিয়ে কোনো অসুবিধা নেই।

Fig 72



Q is an equivalence relation:

এর চেয়ে বেশী আর করে দেব না, কারণ এই অংকটা একেবারেই Example 60-এর দ্বিতীয় অংশের মত। ওখানে 6-এর জায়গায় এখানে 5 বসিয়ে গেলেই হবে।

■

Example 63: Let $\mathbb{Z}^*$ be the set of nonzero integers and let $S = \mathbb{Z} \times \mathbb{Z}^*$, ($\mathbb{Z}$ being the set of integers). Let

$$R = \{x \mid x = ((r,s),(t,u)) \in S \times S \text{ with } ru = st\}.$$

Prove that R is an equivalence relation on S.[3] **(2005)**

SOLUTION: এই অংকটা দেখতে হয়তো একটু গোলমেলে, কিন্তু আসলে খুব জটিল কিছু নয়। এখানে খালি যেটা বুঝতে মাথা গুলিয়ে যেতে পারে সেটা হল set-টা কী আর relation-টাই বা কী। এখানে set-টা হল $S = \mathbb{Z} \times \mathbb{Z}^*$. এর প্রতিটি element-কে দেখতে (a,b)-র মত যেখানে a একটা integer আর b একটা nonzero integer. তার মানে $(1,2),(0,3),(0,-9)$ এরা সবাই এর মধ্যে আছে, কিন্তু $(1,0)$ নেই কারণ দ্বিতীয় সংখ্যাটা শূন্য হতে পারবে না।
এবার আসি relation-টার প্রসঙ্গে। (r,s) আর (t,u) যদি আমাদের set-এর দুটো element হয় তবে তারা R দিয়ে related হবে যদি $ru = st$ হয়, যেমন $\big((1,2),(2,4)\big) \in R$ হবে, কারণ $1 \times 4 = 2 \times 2$. কিন্তু $\big((1,2),(2,5)\big) \notin R$ কারণ $1 \times 5 \neq 2 \times 2$.
গোলমেলে ঠেকছে? আসলে এই relation-টা কিন্তু তোমার ছোটোবেলা থেকেই চেনা। ছোটোবেলায় শিখেছিলে $\frac{1}{2} = \frac{2}{4}$. এখানে খালি $\frac{1}{2}$ না লিখে $(1,2)$ লিখেছে, আর $\frac{2}{4}$ না লিখে লিখেছে $(2,4)$. আর দুটো ভগ্নাংশের "সমান হওয়া"-কে লিখেছে R. কখন বলবে যে $\frac{r}{s} = \frac{t}{u}$? যখন $ru = st$ (দুই দিককে su দিয়ে গুণ করে)। ঠিক এটাই এখানে R-এর সংজ্ঞা। আর সেই কারণেই দ্বিতীয় সংখ্যাটার শূন্য না হওয়া নিয়ে এত কড়াকড়ি, কারণ ওটা তো আসলে fraction-টার denominator.

<u>R is reflexive:</u>
To show $\forall (a,b) \in S \ \big((a,b),(a,b)\big) \in R$
ie, $ab = ab$, which is obviously true.
<u>R is symmetric</u> :
To show $\forall (a,b),(c,d) \in S$

$$\big((a,b),(c,d)\big) \in R \implies \big((c,d),(a,b)\big) \in R,$$

ie, if $ad = bc$, then $cb = da$, which is obviously true.
<u>R is transitive</u> :
To show $\forall (a,b),(c,d),(e,f) \in S$

$$\big[\big((a,b),(c,d)\big) \in R \quad \& \quad \big((c,d),(e,f)\big) \in R\big] \implies \big((a,b),(e,f)\big) \in R,$$

ie, if $ad = bc$ and $cf = de$ then $af = be$.
Take $(a,b),(c,d),(e,f) \in S \times S$ such that $ad = bc$ and $cf = de$.

এখান থেকে "$af = be$"-তে পৌঁছতে একটু অংক কষতে হবে।

$\because b \neq 0, \therefore c = ad/b.$

$\because f \neq 0, \therefore c = de/f.$

Equating, $ad/b = de/f$, or $adf = deb$, or $af = be$, as required since $d \neq 0$.

So R is an equivalence relation on S.

■

Example 64: State true or false with justification: For non-empty set S, $S \times S$ is an equivalence relation on S.[2] **(2005)**

SOLUTION: এই relation-টার মানে হল সবাই সবার সাথে related. অর্থাৎ যত রকম তীর আঁকা যায় সবই আঁকা হয়েছে। কয়েকটা উদাহরণ দেখানো হয়েছে Fig 72-এ। যদি S-এ খালি একটাই element থাকে তবে খালি একটাই তীর আঁকা যায়, সুতরাং এক্ষেত্রে $S \times S$ relation-টা হবে Fig 72(i)-এর মত। যদি S-এ খালি দুটো element থাকে তবে $S \times S$ দেখতে হবে Fig 72(ii)-এর মত। একইভাবে Fig 72(iii)-এ দেখানো হয়েছে S-এ তিনটে element থাকলে কী হত। এর চেয়ে বড় S-এর ক্ষেত্রে ছবি আঁকতে গেলে ভীষ্মের শরশয্যার মত দেখাবে।
সুতরাং এটা যে reflexive, symmetric transitive তিনটেই হবে তাতে আশ্চর্যের কিছু নেই, কারণ কোনো তীরই তো আর বাদ নেই, যেখানে যা চাইবে সব পাবে।

Reflexive :

Because $\forall s \in S \quad (s, s) \in S \times S.$

Symmetric:

Because $\forall s, t \in S \quad (s, t), (t, s) \in S \times S.$

So trivially $(s, t) \in S \times S \implies (t, s) \in S.$

Transitive:

If we take $s, t, u \in S$ such that $(s, t), (t, u) \in S \times S$, then clearly $(s, u) \in S \times S$, because $s, u \in S$.

Hence $S \times S$ is an equivalence relation.

■

Exercise 34: Prove or disprove:

$$R = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \ : \ 3a + 4b \text{ is divisible by } 7\}$$

is an equivalence relation on $\mathbb{Z}$, where $\mathbb{Z}$ is the set of integers.[3] **(2009.2bi)**

HINT:
এই অংকটা তোমার করার জন্য রেখে দিলাম। খালি একটা জিনিস বলি--লক্ষ কর এখানে a আর b একটু আলাদাভাবে রয়েছে, a রয়েছে $3a$ আকারে, কিন্তু b রয়েছে $4b$ আকারে। সুতরাং symmetry নিয়ে সন্দেহ জাগা স্বাভাবিক। পরীক্ষা করেই দ্যাখো!
■

একইরকম আরেকটা অংক।

Exercise 35: A relation ρ is defined on $\mathbb{Z}$ (set of integers) by "$x\rho y$ if and only if $4x+7y$ is divisible by 11" for $x, y \in \mathbb{Z}$. Show whether ρ is an equivalence relation on $\mathbb{Z}$.[3] ■

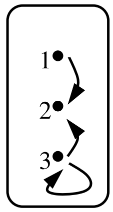


Fig 73

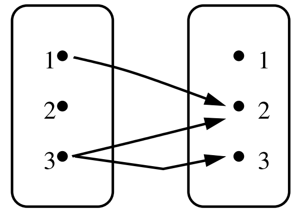


Fig 74

8.3 Properties

Example 65: Prove that a relation ρ defined on a set A is an equivalence relation if and only if ρ is reflexive and $a\rho b$, $b\rho c$ together imply $c\rho a$ for $a, b, c \in A$. **(2008)**

SOLUTION: এটা একটা "if and only if" অংক। তাই দুটো অংশ থাকবে। প্রথমে "If"-টা করি--

> If part: We are given:
>
> 1. ρ is reflexive, i.e, $\forall a \in A \quad a\rho a$.
> 2. $\forall a, b, c \in A \quad [a\rho b \quad \& \quad b\rho c] \implies c\rho a$.
>
> To show: ρ is an equivalence.

Equivalence দেখানো মানে তিনটে জিনিস দেখানো-- reflexive, symmetric আর transitive. তার মধ্যে প্রথমটা তো দেওয়াই আছে।

> Reflexive: Given.

Symmetry আর transitivity আলাদা করে দেওয়া নেই, ওরা ওই দ্বিতীয় শর্তটার মধ্যে একসঙ্গে মিশে আছে। আমাদের কাজ ওদেরকে আলাদা করে বার করে আনা।

> Symmetric: To show
>
> $\forall x, y \in A \quad (x\rho y \implies y\rho x)$.
>
> $\forall x, y$ Take any $x, y \in A$ with $x\rho y$.
>
> Then, by reflexivity, $x\rho x$.
>
> Taking $a = b = x$ and $c = y$ in condition 2 we have $y\rho x$, as required.

সবশেষে transitivity-র পালা--

> Transitive: To show
>
> $\forall x, y, z \in A \quad ([x\rho y \ \& \ y\rho z] \implies x\rho z)$.
>
> $\forall x, y, z$ Take any $x, y, z \in A$ with $x\rho y$ and $y\rho z$.

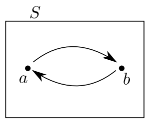


Fig 75

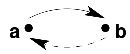


Fig 76

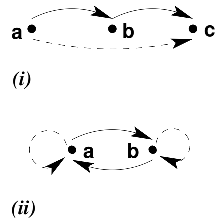


Fig 77

Taking $a = x, b = y$ and $c = z$ in condition 2, we have $z\rho x$.
So, by symmetry of ρ, we have $x\rho z$, as required.

এবার অন্য দিকটা--

<u>Only if part:</u> We are given ρ is an equivalence.
So, by definition, ρ is reflexive.
To show

$$\forall a, b, c \in A \quad ([a\rho b \quad \& \quad b\rho c] \implies c\rho a).$$

$\forall a, b, c$ Take any $a, b, c \in A$ with $a\rho b$ and $b\rho c$.

Then, by transitivity, $a\rho c$.
So, by symmetry, $c\rho a$, as required.

■

Example 66: Prove or set a counterexample to disprove the statement "The union of two equivalence relations is again an equivalence relation".[3] **(2010.2bii)**

Solution:

<u>Counterexample:</u>
Let $S = \{1, 2, 3\}$.
Let $R_1 = \{(1,1), (2,2), (3,3), (1,2), (2,1)\}$
and $R_2 = \{(1,1), (2,2), (3,3), (2,3), (3,2)\}$.
Then R_1 and R_2 are both equivalences.
But

$$R_1 \cup R_2 = \{(1,1), (2,2), (3,3), (1,2), (2,1), (2,3), (3,2)\}$$

is not an equivalence, because it is not transitive.

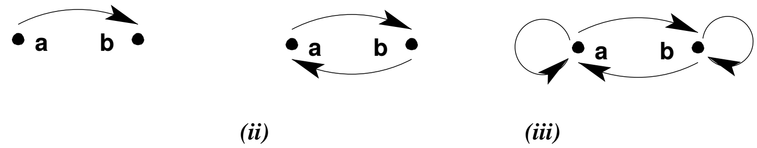


Fig 78

⟦ Because:

$(1,2),(2,3) \in R_1 \cup R_2$ but $(1,3) \notin R_1 \cup R_2$.

⟧

বলতে পারো, কী করে এই counterexample-টা বানালাম? মনে রেখো যে, equivalence মানেই দলাদলি। তাই আমরা S-কে দুইভাবে দলে-দলে ভেঙেছি, খালি একটা জিনিস মাথায় রেখে--প্রথম দলগুলোর মধ্যে একটা দল যেন দ্বিতীয় দলগুলোর বেলায় ভেঙে যায়। যেমন, আমাদের উদাহরণে প্রথমভাবে ভেঙেছিলাম $S = \{1,2\} \cup \{3\}$ হিসেবে, আর দ্বিতীয়ভাবে ভেঙেছিলাম $S = \{1\} \cup \{2,3\}$ হিসেবে। প্রথমবারের $\{1,2\}$ দলটা দ্বিতীয়বারে ভেঙে গেছে, কারণ 1 আর 2 আলাদা আলাদা দলে রয়েছে। ব্যস্, অমনি এই দুটো equivalence-এর union আর equivalence থাকবে না। ■

নীচের অংকটা একইরকম, খালি এবার union-এর জায়গায় intersection.

Exercise 36: Prove or set a counterexample to disprove the statement "The intersection of two equivalence relations is again an equivalence relation". ■

8.4 Relation-এর domain আর range

Function-এর যেমন domain আর range হয় তেমনি relation-দেরও হয়। সেটা বোঝার জন্য Fig 73 দ্যাখো। এখানে আমরা একটা relation-কে তীর চিহ্ন এঁকে দেখিয়েছি। এই ছবিটা একটু অন্যভাবেও আঁকা যেত, Fig 74-এর মত করে। এখানে set-টা দুবার এঁকেছি, এবং তীর চিহ্নগুলো সবাই প্রথম set-টা থেকে শুরু হয়ে দ্বিতীয় set-এ গিয়ে শেষ হয়েছে। এতে ছবিটা খানিকটা function-এর মত দেখতে হয়েছে, যদিও এটা মোটেই একটা function নয়। কারণ লক্ষ কর যে, 2 থেকে কোনো তীর বেরোয় নি, এবং 3 থেকে একাধিক তীর বেরিয়েছে। যে সব বিন্দু থেকে তীর বেরিয়েছে তাদের set-টাকে বলে relation-টার domain, আর যে সব বিন্দুতে তীরগুলো শেষ হয়েছে তাদের set-টাকে বলে relation-টার range. আমাদের উদাহরণে domain হল $\{1,3\}$ আর range হল $\{2,3\}$.

Example 67: Find the domain and range of the binary relation

$$P = \{(x,y) \mid 2x + y = 41; \quad x, y \in \mathbb{N}\},$$

where $\mathbb{N}$ denotes the set of natural numbers.[2] **(2010.2bi)**

SOLUTION:

If $(x,y) \in P$ then $2x + y = 41$ and so y must be odd and $1 \le y \le 39$.

For each such y there is unique $x \in \mathbb{N}$ given by

$$x = \frac{41 - y}{2}$$

> such that $(x, y) \in P$.
> Thus x can take any value in the set $\{1, ..., 20\}$.
> So the domain of P is $\{1, ..., 20\}$, and range of P is $\{1, 3, 5, ..., 39\}$.

■

DAY 9
Relation (part 2)

9.1 ইচ্ছে মত relation তৈরী

Example 68: Give an example (with justification) of a relation which is symmetric but neither reflexive nor transitive. **(2000,2006)**

SOLUTION: খুব সহজ একটা set নেওয়া যাক--

> Take $S = \{a, b\}$.

এবার কিছু তীরচিহ্ন বসাতে হবে।

- যেহেতু symmetric চেয়েছে, তাই ধরো a থেকে b-তে, এবং b থেকে a-তে তীর বসালাম। Fig 75 দ্যাখো।
- এটা reflexive যে নয়, সে তো দেখতেই পাচ্ছো, কারণ a থেকে a-তে কোনো তীর নেই।
- একই ভাবে transitive-ও নয়, কারণ a থেকে b-তে তীর আছে, আবার b থেকে a-তে তীর আছে, অথচ a থেকে a-তে তীর নেই।

ছবির বক্তব্যটাকে লিখে প্রকাশ করা যাক--

> Take the relation
> $$R = \{(a, b), (b, a)\}.$$

এবার লিখে দিই কেন এই R-দিয়ে কাজ চলবে--

> R is not reflexive because $(a, a) \notin R$.
> R is symmetric because R consists of only (a, b) and (b, a).
> R is not transitive because $(a, b), (b, a) \in R$ but $(a, a) \notin R$.

■

Example 69: State true or false with justification: If ρ is a symmetric and transitive relation

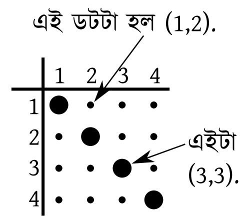


Fig 79

on a set S, then ρ is a reflexive relation.[2] **(1999)**

SOLUTION: এই অংকটা একটা বহুলপ্রচলিত ঠকানো প্রশ্ন। আমরা জানি যে equivalence relation-এর definition-এ তিনটে জিনিস লাগে--symmetry, transitivity আর reflexivity. যদি প্রথম দুটো থেকেই তৃতীয়টা পাওয়া যেত, তবে নিশ্চয়ই লোকে equivalence relation-এর definition-এ কষ্ট করে তিনটে জিনিস আলাদা করে উল্লেখ করত না, খালি symmetry আর transitivity বলেই ছেড়ে দিত। সুতরাং অনুমান করা যাচ্ছে যে, বোধহয় statement-টা true নয়। কিন্তু অনুমান করলেই খালি হবে না, দস্তুরমত একটা counterexample খাড়া করা চাই, যেখানে এমন একটা relation দেখাতে পারি যেটা symmetric, transitive কিন্তু reflexive নয়।

এরকম একটা relation বার করার আগে চট্ করে মনে করে নিই যে, symmetric আর transitive মানে কি ছিল। যদি আমরা একটা relation-কে তীর চিহ্ন দিয়ে দেখাই তবে symmetric মানে-- a থেকে b-তে তীর থাকলে b থেকে a-তে উল্টো তীরটাও থাকতে বাধ্য (Fig 76-এ যেটা ড্যাশ-ড্যাশ দিয়ে দেখানো হয়েছে)। আর transitive মানে হল যদি দুটো তীর পরপর থাকে তবে প্রথমটার গোড়া থেকে দ্বিতীয়টার ডগা পর্যন্ত আরেকটা তীর থাকবেই। এই প্রসঙ্গে যে চিত্রটা মনে ভেসে ওঠে সেটা Fig 77(i)-এর মত। কিন্তু ভুলে গেলে চলবে না যে পরপর তীরদুটো Fig 77(ii)-র মত পরস্পরের বিপরীতেও হতে পারে। সেক্ষেত্রে transitivity-র জন্য দুমাথায় দুটো loop লাগবে। এই loop-গুলো এই অংকে বিশেষ গুরুত্বপূর্ণ কারণ reflexive মানে প্রত্যেক বিন্দুতেই এরকম একটা করে loop আছে। আমরা এমন একটা relation খুঁজছি যেটা reflexive নয়, সুতরাং আমরা এই loop-গুলোকে এড়িয়ে চলতে চাইব, আমরা চাইব যেন অন্ততঃ একটা বিন্দুতে এরকম loop না থাকে। এই কটা কথা মনে রেখে এবার counterexample খোঁজা আরম্ভ করি। কিছু একটা থেকে তো শুরু করতে হবে, ধরো a থেকে b-তে একটা তীর এঁকে শুরু করি (Fig 78(i))। যেহেতু symmetric চাই, সুতরাং b থেকে a-তে একটা তীর না দিয়ে পথ নেই (Fig 78(ii))। আর যেই সেটা দেব অমনি transitivity এসে a আর b-তে দুটো loop বসিয়ে দেবে (Fig 78(iii))। যাঃ, আমরা না loop-গুলোকে এড়িয়ে চলতে চাইছিলাম? একখানা তীর বসাতে না বসাতেই যে দু দুটো loop উড়ে এসে জুড়ে বসল! এভাবে যেখানেই তীর আঁকব সেখানেই তো loop গজিয়ে উঠবে। কী করা যায়?

এর হাত থেকে রক্ষা পাবার উপায়টা খুবই সোজা, কিন্তু এত সোজা যে মাথায় আসতে চায় না। উপায়টা হল কোনোই তীর না আঁকা! খাবি খেও না! তীর যে আঁকতে হবেই এমন তো কেউ মাথার দিব্যি দেয় নি! কোনো তীর না আঁকা মানে কারো সঙ্গে কেউ related নয়। সেটাও তো একটা relation, যাকে বলে empty relation.

মনে রেখো যে একটা nonempty set S-এর ওপরে একটা relation মানে $S \times S$-এর যেকোনো একটা subset. সুতরাং ϕ-ও একটা relation. এই relation-এ কোনো তীর নেই।

> Let $S = \{1, 2, 3\}$ and $\rho = \phi$.

কিন্তু এখন প্রশ্ন হচ্ছে-- relation-টা symmetric আর transitive হবে তো?

> Then ρ is symmetric because the statement
>
> "$\forall a, b \in S \quad \big((a, b) \in \rho \implies (b, a) \in \rho\big)$"
>
> is <u>vacuously</u> true, since $\nexists a, b \in S$ with $(a, b) \in \rho$.

এখানে ওই "vacuously true" কথাটা লক্ষ কর। এর মানে কী, সেটা আমরা এই অধ্যায়ের গোড়াতে একবার আলোচনা

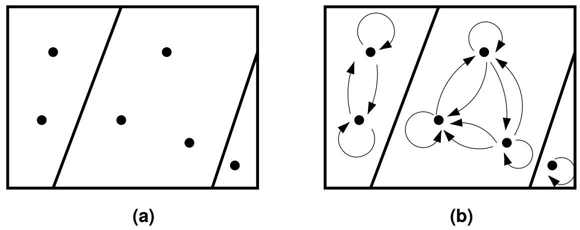


Fig 80

করেছি। মনে করে নেওয়ার জন্য একটা উদাহরণ নিই। ধরো তোমার বাবা কথা দিয়েছেন যে, তুমি পরীক্ষায় ফার্স্ট হলে তোমাকে একটা সাইকেল কিনে দেবেন। অংকের ভাষায়--

"পরীক্ষায় ফার্স্ট $\implies$ সাইকেল"

যদি তুমি সত্যিই ফার্স্ট হও, এবং বাবা তোমাকে সাইকেল কিনে দেন, তবে তাঁর প্রতিজ্ঞা রক্ষা হল। এক্ষেত্রে যদি তিনি সাইকেল না কিনে দিতেন তবে তার প্রতিজ্ঞাটা false প্রমাণিত হত (এবং তুমি বাড়িতে কুরুক্ষেত্র করতে!)। কিন্তু যদি তুমি আদৌ ফার্স্ট না হও তবে? সেক্ষেত্রে বাবা সাইকেল দিন বা না দিন দুই ক্ষেত্রেই তাঁর প্রতিজ্ঞা true থাকছে। কারণ তাঁর প্রতিজ্ঞার গোড়ার শর্তটাই (অর্থাৎ তোমার ফার্স্ট হওয়া) পালিত হয় নি, অতএব তিনি দায়মুক্ত। এই ক্ষেত্রে আমরা বলব যে, তাঁর প্রতিজ্ঞাটা vacuously true. মানে যখন একটা statement হবে এরকম দেখতে--

"কিছু একটা $\implies$ অন্য কিছু একটা"

তখন সেটা vacuously true হবে যদি প্রথম "কিছু একটা"-টাই false হয়ে যায়।
এই যুক্তি অনুসারে আমাদের ρ-টা অবশ্যই symmetric, কারণ symmetry-র definition-এ বলেছে যে, যদি তুমি এমন $a, b \in S$ দেখাতে পারো যেখানে $(a, b) \in \rho$ তবে আমি দেখিয়ে দেব যে $(b, a) \in \rho$. বলাই বাহুল্য যে, তুমি কোনোদিনই এরকম a, b বার করতে পারবে না, কারণ ρ তো বেমালুম ফাঁকা! অতএব আমি দায়মুক্ত, symmetry-টা vacuously true!

> Similarly the statement
>
> "$\forall a, b, c \in S \quad \big((a, b) \in \rho \quad \& \quad (b, c) \in \rho \implies (a, c) \in \rho\big)$"
>
> is vacuously true. So ρ is transitive.

কিন্তু reflexive-এর জন্য কোনো " $\implies$ " লাগে না, তাই সেখানে আর এই vacuously true-র অজুহাতে পার পাওয়া যাবে না।

> But $(1, 1) \notin \rho$. So ρ is not reflexive.

■

এই সমাধানটা ভালো করে বুঝে নাও। তারপর নীচের অংকটা কর দেখি। এটা বস্তুতঃ আগের অংকটারই সামান্য ঠকানো সংস্করণ।

Exercise 37: ধরো $S = \{1, 2, 3\}$. এর উপর এমন একটা nonempty relation দিতে পারো যেটা symmetric এবং transitive, কিন্তু reflexive নয়? ■

এবার কয়েকটা অংক দেখব যেগুলো একটু অন্যরকম। এর জন্য একটা জিনিস মনে রাখলে সুবিধা হবে। যদি একটা set-এ n-খানা element থাকে, তবে তার মোট কতগুলো subset সম্ভব? উত্তর হল--2^n. যেমন যদি $n = 1$ হয়, ধরো $S = \{a\}$, তাহলে তার ঠিক $2^n = 2^1 = 2$-খানাই subset সম্ভব--

$$\phi \text{ আর } \{a\}.$$

যদি $S = \{a, b\}$ নিতাম তবে $n = 2$ হত, এবং সেক্ষেত্রে subset পেতাম $2^n = 2^2 = 4$-টে--

$$\phi, \quad \{a\}, \quad \{b\} \text{ আর } \{a, b\}.$$

এই 2^n-টা কোথা থেকে এল সেটা বোঝা কঠিন নয়। তুমি যখন একটা subset বানাচ্ছ, তখন তুমি n-টা element-এর প্রত্যেকটার ক্ষেত্রে সিদ্ধান্ত নিচ্ছ--ওটাকে তোমার subset-এর মধ্যে রাখবে কিংবা রাখবে না। যদি একটাই element থাকে তবে দুইরকম সিদ্ধান্তের ভিত্তিতে দুটো subset. যদি আরও একটা element থাকে তবে প্রথমবারে যাই সিদ্ধান্ত নাও না কেন, দ্বিতীয় সিদ্ধান্তটাও দু'রকম হতে পারে। সুতরাং মোট subset-এর সংখ্যা দাঁড়াচ্ছে $2 \times 2 = 2^2$. তিনটে element থাকলে তিনবার সিদ্ধান্ত নিতে হচ্ছে তাই $2 \times 2 \times 2 = 2^3$, ইত্যাদি।

এইবার আবার relation-এর প্রসঙ্গে ফেরা যাক। S যদি একটা nonempty set হয়, তবে S-এর উপরে কোনো relation মানে $S \times S$-এর একটা subset. যদি S-এর সাইজ হয় n, তবে $S \times S$-এর সাইজ হবে n^2. সুতরাং যদি প্রশ্ন করি S-এর উপর মোট কতগুলো relation সম্ভব, তবে তার মানে হল $S \times S$-এর কতগুলো subset আছে। এবং এর উত্তরটা হবে 2^{n^2}. নীচের অংকটা এরই সামান্য জটিল সংস্করণ।

Example 70: Find the number of different reflexive relations on a set with n elements.[2] **(2009.2bii)**

SOLUTION:

> Let S be a set with n elements. Then by a relation on S we mean any subset of $S \times S$.
>
> The size of $S \times S$ is n^2.

এই অংকে খালি reflexive relation-দের নিয়ে কাজ করতে বলেছে। সুতরাং আমাদের স্বাধীনতা কম, আমাদের subset-এ অবশ্যই $S \times S$-এর (x, x) জাতীয় element-গুলোকে রাখতেই হবে। এরকম element আছে n-খানা। এইটা বুঝতে যদি অসুবিধা হয় তবে Fig 79 দ্যাখো। এখানে আমরা $S = \{1, 2, 3, 4\}$ নিয়েছি। $S \times S$-এর element-গুলোকে একটা square-এর মত সাজিয়ে ডট্ ডট্ করে এঁকেছি। এখানে (x, x) জাতীয় element-গুলো হল diagonal (কর্ণ) বরাবর ডটগুলো, যেগুলোকে মোটা করে দেখিয়েছি। এই element-গুলোকে আমাদের subset-এ রাখতেই হবে। সুতরাং আমাদের স্বাধীনতা খালি অবশিষ্ট $n^2 - n$-খানা element-এর বেলায়।

> Since we need a reflexive relation, the subset must contain all the n elements of the form (x, x) for $x \in S$.
>
> It may or may not contain any of the remaining $n^2 - n = n(n-1)$ elements of $S \times S$.
>
> Since the total number of subsets that can be formed using these $n(n-1)$ elements is $2^{n(n-1)}$, hence the required answer is $2^{n(n-1)}$.

■

এই ধরণের অংক করার জন্য ওই ডট্ ডট্ করে ছবি আঁকলে খুব সুবিধা হয়। নীচের অংকগুলো একইরকমের।

Exercise 38: Find the number of different relations that are both reflexive and symmetric on a set with n elements.[2] ■

Exercise 39: Find the number of different symmetric relations on a set with n elements.[2] ■

9.2 Partition

Equivalence আলোচনার সময়ে বলেছিলাম যে, equivalence হল দলাদলির relation. একটা equivalence থাকলেই set-এর element-গুলো দলে দলে ভাগ হয়ে যায়। এইরকম দলে দলে ভাগ হওয়াকে অংকের ভাষায় বলে **partition.** যেমন বঙ্গভঙ্গের সময়ে গোটা বাংলাটাকে ভেঙ্গে বেমালুম দুই টুকরো করে দিয়েছিল! দুটো ভাগের মধ্যে কোনো common জায়গা ছিল না। আবার আগেকার অখণ্ড বাংলার কোনো জায়গা বাদও পড়ল না।

যদি আমরা কলকাতার সব মানুষের set নিই, তবে তাকে আমরা নানাভাবে partition করতে পারি। বয়স দিয়ে, যেমন, 20 বছর পর্যন্ত একটা দলে, 20 থেকে 30 পর্যন্ত আরেকটা দলে, আর বাকীরা একটা তৃতীয় দলে। এটা একটা partition, কারণ এতে কেউ বাদ গেল না, আবার কেউই একাধিক দলভুক্ত হল না।

আবার আরেকভাবে partition করা যেত এইভাবে--যাদের বিয়ে হয় নি তারা এক দলে, যারা বিবাহিত তারা দ্বিতীয় দলে, আর বাকীরা (ডিভোর্সী ইত্যাদি) তারা তৃতীয় দলে।

কিন্তু যদি বলতাম সব মেয়েরা এক দলে আর সব বাঁহাতিরা আরেকটা দলে, তবে সেটা partition হত না, কারণ এতে ডানহাতি ছেলেগুলো বাদ পড়ে গেল, আবার বাঁহাতি মেয়েগুলো দুদলেই ঢুকে পড়ল।

Example 71: State true or false with justification: If $S = \{1, 2, 3, ..., 10, 11, 12\}$, then the sets ϕ (null set) $\{1, 3, 5, 8\}$, $\{2, 4, 6, 9\}$, $\{5, 9, 11, 12\}$, form a partition of S.[2] **(2004)**

SOLUTION:

> The statement is false,
> because $\{5, 9, 11, 12\} \cap \{1, 3, 5, 8\} = \{5\} \neq \phi$.

■

Equivalence মানেই যেহেতু দলাদলির relation, তাই বুঝতেই পারছ যে, equivalence-এর সঙ্গে partition-এর গলাগলি সম্পর্ক। যে কোনো partition থেকেই আমরা একটা equivalence relation বানাতে পারি। যেমন বঙ্গভঙ্গের উদাহরণে এই equivalence relation-টা হবে "দেশোয়ালী ভাই" relation, অর্থাৎ xRy মানে হয় x, y দুজনেই ঘটি, নয় দুজনেই বাঙাল।

আবার বিপরীতপক্ষে যে কোনো equivalence-এর ফলেই একটা partition-এর জন্ম হয়।

Fig 80-এর উপরের ছবিতে একটা partition দেখানো হয়েছে। আর নীচের ছবিটায় দেখিয়েছি তার পিছনে যে equivalence-টা আছে, সেটা। লক্ষ কর একই দলের মধ্যে সবার সঙ্গে সবার সম্পর্ক আছে, কিন্তু দুটো বিভিন্ন দলের লোকেদের মধ্যে মুখ দেখাদেখি নেই।

9.2.1 Partition থেকে equivalence

এবার আমরা দেখব একটা partition দেওয়া থাকলে কী করে তা থেকে একটা equivalence পেতে হয়।

Example 72: Prove that a partition of a nonempty set S determines an equivalence relation on S.[3] **(2001,2004,2006)**

SOLUTION:

> Let
> $$S = \bigcup_{i\in I} S_\alpha$$
> be a partition of S, where I is some index set.

এইটা দেখে খাবি খেয়ো না। একটু বুঝে নেওয়া যাক। যদি partition-এ খালি দুটো set থাকত তবে আমরা লিখতাম $S = S_1 \cup S_2$. কিন্তু 10-টা set থাকলে এভাবে লিখতে হাত ব্যথা হয়ে যেত, তাই তখন লিখতাম

$$S = S_1 \cup S_2 \cup \cdots \cup S_{10}.$$

এটাও লিখতে বেশ কষ্ট, বিশেষ করে ওই বার বার S লেখাটা। তাই আরো সহজে লিখব

$$S = \bigcup_{i\in\{1,...,10\}} S_i.$$

এখানে i হল S_i-এর index. যেহেতু এই i এখানে 1 থেকে 10 পর্যন্ত value নিতে পারে, তাই $\{1,...,10\}$-কে বলব index set.
আমাদের অংকে আমরা যেকোনো partition নিয়ে কাজ করছি। সুতরাং index set-এ যতখুশী element থাকতে পারে। তাই আমরা index set-টা যেকোনো set নিয়েছি I. খালি মনে রাখা দরকার যে S_i-গুলো যেন একটার ঘাড়ে একটা গিয়ে না পড়ে--

> Thus, $\forall i \neq j \in I$ we have $S_i \cap S_j = \phi$.

এবার আমরা relation-টা লিখব-- $x \sim y$ হবে যদি দুজনেই একই দলভুক্ত হয় (মানে একই S_i-র ভিতরে দুজনেই থাকে)।

> We define a relation $\sim$ on S as follows:
>
> For $a, b \in S$ we shall say $a \sim b$ if and only if $\exists i \in I \quad a, b \in S_i$.

এই বার দেখাতে হবে যে এই relation-টা সত্যই একটা equivalence relation, মানে ওই তিনটে শর্ত পরীক্ষা করে দেখতে হবে--reflexivity, symmetry আর transitivity.

> Shall show that $\sim$ is an equivalence relation.

প্রথমে reflexivity. এটা প্রায় বলাই বাহুল্য।

> <u>Reflexivity:</u> To show
>
> $\forall a \in S \quad a \sim a.$
>
> $\boxed{\forall a}$ Take any $a \in S$.
>
> $\because S = \cup_{i\in I} S_i$,
>
> $\therefore \exists i \in I \quad a \in S_i$.
>
> $\therefore a \sim a$, as required.

Symmetry দেখানো একই রকম সোজা--

Symmetry: To show

$$\forall a, b \in S \quad (a \sim b \implies b \sim a).$$

$\boxed{\forall a, b}$ Take any $a, b \in S$ with $a \sim b$.

Then $\because a \sim b \therefore \exists i \in I \quad a, b \in S_i$,
$\therefore b, a \in S_i$,
$\therefore b \sim a$, as required.

এবার transitivity. একই রকম যুক্তি এক্ষেত্রেও প্রযোজ্য।

Transitivity: To show

$\forall a, b, c \in S \quad ([a \sim b \ \& \ b \sim c] \implies a \sim c)$.

$\boxed{\forall a, b, c}$ Take any $a, b, c \in S$ with $a \sim b$ and $b \sim c$.

Now, $\because a \sim b$, $\therefore \exists i \in I \quad a, b \in S_i$.
Also, $\because b \sim c$, $\exists j \in I \quad b, c \in S_j$.
Thus, $b \in S_i \cap S_j$.

এ থেকে আমরা সিদ্ধান্ত করব যে $i = j$. কারণ, যদি $i \neq j$ হত, তবে আমরা জানি যে $S_i \cap S_j = \phi$ হত। কিন্তু এখানে দেখা যাচ্ছে যে $S_i \cap S_j$-র মধ্যে b রয়েছে। সুতরাং--

So $i = j$, because otherwise $S_i \cap S_j = \phi$.
So $c \in S_i$. Since $a, c \in S_i$, we have $a \sim c$, as required.

■

এই যে যুক্তিটা শিখলাম, সেটাই নীচের অংকটায় হাতেকলমে করতে বলেছে একটা উদাহরণের জন্য।

Example 73: Consider the set $S = \{1, 2, 3, 4\}$ and the partition

$$\{\{1\}, \{2\}, \{3, 4\}\}$$

of S. Find the equivalence relation corresponding to this partition of S.[3] **(2011.14ii)**
SOLUTION:

Let the partition be denoted by $\{S_1, S_2, S_3\}$, where

$$S_1 = \{1\}, \quad S_2 = \{2\}, \quad S_3 = \{3, 4\}.$$

We know that the corresponding equivalence relation is given as follows.
If $a, b \in S$ then $a \sim b$ if and only if a, b both belong to same S_i.

> Thus here 1 is related only with 1. Similarly, 2 is related only with 2. Also, 3 is related with only 3, 4. Similarly 4 is related with only 3, 4.
> So the required relation is
> $$R = \{(1,1),(2,2),(3,3),(3,4),(4,3),(4,4)\}.$$

■

9.2.2 Equivalence থেকে partition

একটা partition থেকে যেমন একটা equivalence relation পাওয়া যায়, তেমনি একটা equivalence relation থেকে আবার একটা partition পাওয়া যায়। আরেকভাবে বলতে গেলে partition আর equivalence relation হল একই জিনিসের দুটো বর্ণনা। একটা জানলেই অন্যটা জানা যায়। নীচের অংকগুলোতে আমরা সেটাই করব--একটা equivalence থেকে শুরু করে ধাপে ধাপে একটা partition-এর দিকে এগোব। ব্যাপারটা এইরকম--ধরো একটা set আছে A আর তার উপর একটা equivalence আছে ρ. এর ফলে A-টা দলে দলে ভাগ হয়ে যাবে। এককেটা দলকে বলব এককেটা equivalence class. যেমন $a \in A$ হলে a-র equivalence class হবে $\{b \in A \;:\; (a,b) \in \rho\}$. এরকম যাবতীয় equivalence class-গুলো মিলেই A-র একটা partition হবে। সেটাই ধাপে ধাপে দেখাবো আমরা। প্রথম অংকটায় দেখাব যে, দুটো আলাদা আলাদা equivalence class সর্বদা disjoint হয়।

Example 74: Let ρ be an equivalence relation on a set A and $a, b \in A$ such that $(a,b) \notin \rho$.

Prove that $cl(a)$ and $cl(b)$ are disjoint. (Here $cl(a)$ means the equivalence class containing a determined by ρ.)[2] **(2002)**

SOLUTION: ধরো ইস্টবেঙ্গল মোহনবাগান খেলা হচ্ছে। S হচ্ছে যাবতীয় দর্শকের set. আমি এই set-এর ওপরে একটা equivalence relation ρ দিচ্ছি এইরকম--$(x,y) \in \rho$ মানে x এবং y একই দলের সমর্থক, বা দুজনেই নিরপেক্ষ। এই equivalence relation-এর ভিত্তিতে যাবতীয় দর্শককে তিনটে দলে ভাগ করা যাবে-- মোহনবাগানের সমর্থক, ইস্টবেঙ্গলের সমর্থক এবং নিরপেক্ষ। এইটা S-এর একটা partition.

ধর তুমি একজন দর্শক, a. তাহলে তুমি এই তিনটে ভাগের কোনো একটাতে আছো। তোমার ভাগটাকে বলব তোমার equivalence class. এই অংকে একে লেখা হয়েছে $cl(a)$. যেমন a ইস্টবেঙ্গলের সমর্থক হলে $cl(a)$ হবে যাবতীয় ইস্টবেঙ্গলের সমর্থকদের set.

এই অংকে দেখাতে হবে যে দুটো লোক যদি equivalent না হয় (অর্থাৎ দুজনেই একই দলের সমর্থক বা দুজনেই নিরপেক্ষ না হয়), তবে দুজনে আলাদা আলাদা ভাগে পড়বে। এমনিতে এটা প্রায় বলাই বাহুল্য, খালি অংকের ভাষায় গুছিয়ে লেখার অপেক্ষা।

আমরা এখানে দেখাতে চলেছি যে $cl(a) \cap cl(b) = \phi$. কোনো set-কে ϕ দেখানোর একটা কায়দা হল contradiction লাগানো।

> Let, if possible, $cl(a) \cap cl(b) \neq \phi$.

ধর a হচ্ছ তুমি, ইস্টবেঙ্গলের ঘোর সমর্থক, আর b হলাম আমি, নিরপেক্ষ শান্তিপ্রিয় ভদ্রলোক। আমরা এক্ষুণি ধরে নিয়েছি যে, তোমার ভাগ $cl(a)$ এবং আমার ভাগ $cl(b)$-র মধ্যে কিছুটা intersection আছে। তার মানে এমন দর্শক আছে, যে তোমারও ভাগে, আমারও ভাগে। তার মানে সে ইস্টবেঙ্গলের সমর্থক, আবার এদিকে নিজেকে নিরপেক্ষ বলেও দাবী করছে! সেটা তো অসম্ভব!

> Pick any $c \in cl(a) \cap cl(b)$.

ইনিই সেই দুমুখো ভদ্রলোক। তোমার যা মত এনারও তাই মত, আবার আমার যা মত সেটাও ওনার মত--

> Then $(a,c) \in \rho$ and $(b,c) \in \rho$.

আমার যা মত ওনার তাই মত, অর্থাৎ কিনা, ওনার যা মত আমারও তাই মত। একই কথাকে ঘুরিয়ে দুবার করে বলাটা বোকা বোকা লাগতে পারে, কিন্তু অংকের ভাষায় এটা গুরুত্বপূর্ণ ধাপ, কারণ এখানেই আমরা symmetry লাগাচ্ছি।

> So, by symmetry of ρ, we have $(c,b) \in \rho$.

এই বার contradiction-টা--

> So, by transitivity of ρ, we have $(a,b) \in \rho$ $(\Rightarrow\Leftarrow, \because (a,b) \notin \rho)$.

■

আমরা এই অংকে দেখলাম যে, a আর b যদি পরস্পরের সাথে সম্পর্কিত না হয়, তবে ওদের equivalence class-দুটো disjoint. কিন্তু যদি ওরা সম্পর্কিত হয়? সেক্ষেত্রে ওদের equivalence class দুটো একই হবে। সেটা একটু চিন্তা করলেই বোঝা যায়। এর উল্টো দিকটাও ঠিক, যদি a আর b-এর equivalence class দুটো একই হয়, তবে ওরা পরস্পরের সাথে সম্পর্কিত হতে বাধ্য। এই দুটো দিকই দেখাতে বলেছে নীচের অংকটায়।

Example 75: Let R be an equivalence relation on a nonempty set S and $a, b \in S$. Prove that $[a] = [b]$ if and only if aRb. Here

$$[a] = \{x \in S | xRa\}.$$

[5] **(2005)**

SOLUTION:

> To show: $[a] = [b] \iff aRb$.

দুই ধাপে ভেঙে দেখাব, প্রথমে $\implies$ তারপর $\impliedby$.

> Step 1: $[a] = [b] \implies aRb$:
>
> Since R is reflexive, hence $a \in [a] = [b]$.
>
> Hence, by definition of $[b]$, we have aRb, as required.

এবার উল্টো দিকটা--

> Step 2: $[a] = [b] \impliedby aRb$.

এখানে $[a]$ আর $[b]$ হল দুটো set. ওদের সমান দেখানোর জন্য প্রথমে দেখাব $[b] \subseteq [a]$ এবং তারপর দেখাব $[a] \subseteq [b]$.

> Take any $b' \in [b]$.
>
> Then bRb'.
>
> $\because aRb$, and R is transitive,
>
> $\therefore aRb'$.
>
> So $b' \in [a]$.

> Thus $[b] \subseteq [a]$.

এবার $[a] \subseteq [b]$ দেখানোর পালা। নতুন করে কিছু করার নেই--

> Again, since R is symmetric, bRa. Hence by similar argument as above, $[a] \subseteq [b]$.
> Combining, $[a] = [b]$, as required.

■

এই কয়টা অংকে কী কী শিখলাম সেটা একটা উদাহরণ নিয়ে বুঝে রাখি।

Example 76: ধরো $S = \{1, 2, ..., 7\}$. এর উপরে একটা equivalence relation দিলাম এইরকম--aRb বলব যদি $a - b$-টা 3 দিয়ে ভাগ যায়। তাহলে S-এর বিভিন্ন element-এর equivalence class-গুলো কী কী হবে?

SOLUTION: প্রথমে 1-এর equivalence class বার করি। এটা হল সেই সব $b \in S$-এর set, যাদের জন্য $1 - b$-টা 3 দিয়ে ভাগ যাবে, মানে সেই সব b যাদের 3 দিয়ে ভাগ করলে ভাগশেষ আসবে 1. তাই

$$[1] = \{1, 4, 7\}.$$

একইভাবে

$$\begin{aligned}
[2] &= \{2, 5\} \\
[3] &= \{3, 6\} \\
[4] &= \{1, 4, 7\} \\
[5] &= \{2, 5\} \\
[3] &= \{3, 6\} \\
[7] &= \{1, 4, 7\}.
\end{aligned}$$

লক্ষ কর যে, এই যে সাতটা set পেলাম $[1], ..., [7]$, এর মধ্যে কিন্তু আসলে তিনটে set-ই আলাদা আলাদা, এরা হল $\{1, 4, 7\}$, $\{2, 5\}$ আর $\{3, 6\}$. এবং এরা মিলে S-এর একটা partition হচ্ছে। এদের মধ্যে এমন কোনো দুটো set নেই যারা খানিকটা overlap করেছে, হয় পুরো এক, যেমন $[1], [4]$ আর $[7]$, আর নয়তো সম্পূর্ণ disjoint, যেমন $[1]$ আর $[2]$. ■

নীচের অংক দুটোতে নতুন কোনো বক্তব্য নেই, ওই একই জিনিস দেখাতে বলেছে।

Exercise 40: If $cl(a)$ is an equivalence class and $b \in cl(a)$ then prove that $cl(b) = cl(a)$. **(2008)**

HINT:
এটা একটা equivalence relation-এর অংক, কিন্তু equivalence relation-টার কোনো নাম দেওয়া হয় নি। একটা নাম থাকলে উত্তরটা লিখতে সুবিধা হবে। তাই আমরাই একটা নাম দিয়ে নিই--

> Let ρ be the equivalence relation.

এর পর থেকে কী করতে হবে সেটা তো একটু আগেই শিখলাম। ■

Example 77: Let ρ be an equivalence relation on a set S and $a, b \in S$. Prove that $cl(a)$ and $cl(b)$ are identical or disjoint.[3] **(2011.15i)**

SOLUTION: আবার একই রকম একটা অংক। এখানে বলেছে $cl(A)$ আর $cl(b)$ হয় একই আর নয়তো সম্পূর্ণ disjoint. এরকম "হয় এটা নয়তো ওটা" জাতীয় জিনিস প্রমাণ করার জন্য "ওটা না হলে এটা" প্রমাণ করলে সুবিধা হয়। এখানে তাই আমরা দেখাব যে, $cl(a)$ আর $cl(b)$ যদি disjoint না হয়, তবে ওরা identical হতে বাধ্য।

> Let $cl(a)$ and $cl(b)$ be not disjoint, ie $cl(a) \cap cl(b) \neq \phi$.
> Shall show $cl(a) = cl(b)$.

সেই দুই ধাপের কায়দাটা লাগাব, মানে $cl(a) \subseteq cl(b)$ আর $cl(b) \subseteq cl(a)$ দেখাব।

> Take any $a' \in cl(a)$.
> Then $a' \rho a$.
> $\because cl(a) \cap cl(b) \neq \phi, \ \therefore \exists c \in cl(a) \cap cl(b)$.
> So $a \rho c$ and $c \rho b$.

আমাদের হাতে তাহলে আছে $a' \rho a$, $a \rho c$ আর $c \rho b$. দিব্যি পরপর ফিট করে যাচ্ছে, সুতরাং--

> $\therefore$By transitivity, $a' \rho b$, ie, $a' \in cl(b)$.
> Hence $cl(a) \subseteq cl(b)$.

এবার $cl(b) \subseteq cl(a)$ দেখানোর পালা। কিন্তু সেখানে আর নতুন করে কিছু দেখানোর নেই, a আর b-এর স্থানবিনিময় করে দিলেই হল--

> By interchanging a, b above, we also get $cl(a) \subseteq cl(b)$.
> Hence $cl(a) = cl(b)$, as required.

■

উপরের অংকগুলোতে যা যা শিখলাম, সেসব মিলিয়ে নীচের অংকটা।

Example 78: Prove that an equivalence relation on a set S determines a partition of S.[3] **(2013)**

SOLUTION: এই উত্তরটা পড়ার আগে হয়তো Example 76-এর সহজ উদাহরণটা দেখে নিলে সুবিধা হবে।

> Let ρ be an equivalence relation on S.
> For $a \in S$ we define its equivalence class $cl(a) = \{s \in S \ : \ a \rho s\}$.
> Then for any $a, b \in S$ we have either $cl(a) = cl(b)$ or $cl(a) \cap cl(b) = \phi$.
>
> ⟦ <u>Because:</u>

এইটা আমরা আগের অংকটাতেই দেখিয়েছি। সেই উত্তরটা হুবহু এখানে ঢুকিয়ে দাও।

>]]
> Now let the set of all distinct equivalence classes be $\{S_i \ : \ i \in I\}$.

Example 76-এর বেলায় যেমন সাতটা equivalence class-এর মধ্যে আসলে খালি তিনটে set-ই ঘুরে ফিরে আসছিল। তাই সেই উদাহরণে আমরা $S_1 = \{1,4,7\}$, $S_2 = \{2,5\}$ আর $S_3 = \{3,6\}$ নিতে পারতাম। তিনটে set হল, তাই $I = \{1,2,3\}$ হত। এইখানে ছোট্টো করে বলে রাখি যে, এরকমভাবে যে সব সময়েই নেওয়া যাবে সেটাকে বলে axiom of choice. কিন্তু সেই ব্যাপারটা এই বইয়ের পক্ষে বড্ড বেশী ভারী জিনিস, তাই সমাধানের মধ্যে সেটা আর উল্লেখ করলাম না। এবার দেখাব যে, S_i-গুলো মিলে S-এর একটা partition হয়। তার জন্য দুটো জিনিস দেখাতে হবে--

- এক, S_i-গুলো disjoint. সেটা তো দেখালামই।
- $S = \cup_{i \in I} S_i$.

> Then $\forall i \neq j \in I \quad S_i \cap S_j = \phi$.
> Also $S = \cup_{i \in I} S_i$.
>
> [[Because:
>
> If $s \in S$, then $cl(s) = S_j$ for some $j \in I$.
> Hence, by reflexivity, $s \in cl(s) = S_j \subseteq \cup_{i \in I} S_i$.
>
>]]
>
> Thus, $\{S_i \ : \ i \in I\}$ forms a partition of S, as required.

■

Answers

1. $A \cap B$. **2.** $A \cup B$. **3.** বাঁদিকের চাঁদটা হল $A \cap B^c$ বা $A \setminus B$. ডানদিকের চাঁদটা হল $A^c \cap B$ বা $B \setminus A$. **4.** $(A \cap B^c) \cup (A^c \cap B)$. **5.** $(A \cup B)^c$. **6.**

টুকরো	ফর্মুলা
1	$A \cap B \cap C$
2	$A \cap B \cap C^c$
3	$A \cap B^c \cap C$
4	$A^c \cap B \cap C$
5	$A \cap B^c \cap C^c$
6	$A^c \cap B \cap C^c$
7	$A^c \cap B^c \cap C$
8	$A^c \cap B^c \cap C^c$

7. $B = \phi$ নাও, তাহলে $A \cup \phi = \phi$ পাবে, সুতরাং $A = \phi$ হবে। **8.** $B = S \setminus A$ নাও। **11.** ঠিক, ভুল, ঠিক। **12.** না, প্রথম ক্ষেত্রে 1 অব্যবহৃত থাকবে, দ্বিতীয়ক্ষেত্রে 2 থেকে একাধিক তীর চিহ্ন বেরোবে। **18.** $\forall a \in A \quad f^{-ell}(f(a)) = a$, তাই onto. এ থেকে এটাও দেখা যাচ্ছে যে, f হল f^{ℓ}-এর একটা right inverse. **19.** যদি $f^{-r}(b_1) = f^{-r}(b_2)$ হয়, তবে দুদিকে f লাগালেই পাবে $b_1 = b_2$. সুতরাং one-one. যেহেতু $\forall b \in B \quad f(f^{-r}(b)) = b$, তাই f হল f^{-r}-এর একটা left inverse. **20.** হ্যাঁ, $A = \{1\}, B = \{1,2\}$ আর

$f(1) = 1$. **21.** অসম্ভব! **22.** Range of f. **23.** $A = \{1, 2\}$, $B = \{0\}$, $f(1) = f(2) = 0$. এবার $S = \{1\}$ নিলে S^c হবে $\{2\}$. সুতরাং $f(S^c) = \{0\}$. কিন্তু $f(S)^c = \phi$. **24.** Bijection লাগবে, খালি one-one বা onto দিয়ে হবে না। **25.** হ্যাঁ। **26.** ϕ. **28.** $S = \mathbb{N}$ নাও আর $f : S \to S$ নাও এইভাবে-- $f(1) = f(1)$ আর $n \geq 2$-এর জন্য $f(n) = n - 1$. **34.** এটা একটা equivalence. এটা symmetric, কারণ $3a + 4b = 7n$ হলে $3b + 4a = 7(a + b) - (3a + 4b) = 7(a + b - n)$ হবে। একইভাবে reflexive আর transitive-ও হবে। **35.** হ্যাঁ, এটা একটা equivalence. যুক্তিটা ঠিক আগের অংকটার মতই। **36.** ঠিক। **37.** $\{(1, 1)\}$. **38.** $2^{n(n-1)/2}$. **39.** $2^{n(n+1)/2}$.

Chapter II
Group theory (year 1)

DAY 10
গোড়ার কথা

এই বইয়ের বিষয়বস্তু হল modern algebra, যার আরেক নাম abstract algebra. ইংরাজীতে “abstract” মানে "যা ধরা-ছোঁয়া যায় না।" যাকে ধরা-ছোঁয়া যায় না সেরকম জিনিস নিয়ে কাজ করা কতকটা যেন ছায়ার সাথে কুস্তি করার মত ব্যাপার। অনেক ছাত্রই গোড়ায় বুঝে উঠতে পারে না, সেই কাজটা কেন করছি। প্রথমে সেই ব্যাপারটা কিছু উদাহরণ দিয়ে বুঝে নিই।

আজগুবি নয়,
আজগুবি নয়,
সত্যিকারের কথা-
ছায়ার সাথে
কুস্তি করে
গাত্রে হল ব্যথা।

--সুকুমার রায়

Example 1: প্রাচীনকালে গ্রীসদেশে আর্কিমিডিস নামে একজন পণ্ডিত ছিলেন তোমরা জানো। তাঁর নাকি দুটো ফাঁকিবাজ চাকর ছিল। তাদের মধ্যে একটা বোকা, অন্যটা চালাক। এক দিন আর্কিমিডিস তাদের উপর বেজায় চটে গেছেন। কাছেই একটা বাড়ি ছিল, তার সামনে সাতটা থাম ছিল Fig 1-এর মত। আর্কিমিডিস চাকর দুটোকে শায়েস্তা করার জন্য বললেন--যাও, তোমরা ওই থামগুলো ধরে ধরে এক, দুই করে গুণবে। সাত নম্বর থামে পৌঁছে গেলে ফের এক নম্বর থাম থেকে আট, নয় করে গোণা চালিয়ে যাবে। এইভাবে এক হাজার অব্ধি গুণে আমাকে এসে বলবে কোন থামে গোণা শেষ হল। বোকা চাকরটা গুণতে গুণতে জেরবার। কিন্তু চালাক চাকরটা খানিকক্ষণ বিড়বিড় করে কি সব হিসেব করে কিছুমাত্র না গুণে উত্তরটা আর্কিমিডিসকে বলে দিল! কী করে?

SOLUTION: চালাক চাকরটা দেখল যে, প্রতি সাতবারের শেষে নতুন করে এক নম্বর থাম থেকে গোণা শুরু হচ্ছে। সুতরাং যেই থামে 1 গুণছি, সেই থামেই $1+7=8$-ও গুণছি। যেই থামে 2 গুণছি, সেই থামে $2+7=9, \quad 2+2\times 7=16$ ইত্যাদিও গুণছি। সুতরাং উত্তরটা নির্ভর করছে 1000-কে 7 দিয়ে ভাগ করলে কত ভাগশেষ থাকে, খালি তার উপরে। এইবার চট্ করে প্রথম সাতটা সংখ্যা মনে মনে গুণে দেখল যে, ভাগশেষ 1 হলে প্রথম থাম, 2 হলে দ্বিতীয় এইভাবে চলতে চলতে ভাগশেষ 6 হলে ছয় নম্বর থাম পাওয়া যাচ্ছে। আর সাত নম্বর থামের বেলায় ভাগশেষ হচ্ছে 0 (কারণ 7-কে 7 দিয়ে ভাগ

Fig 1

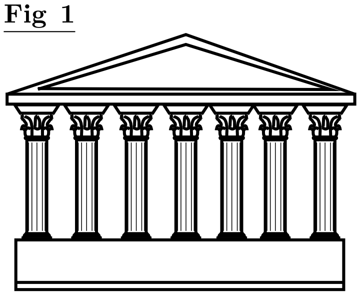
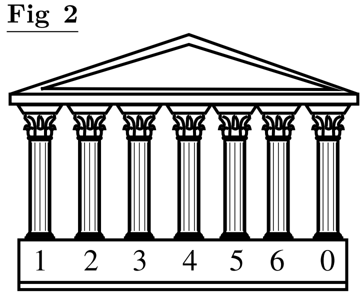


Fig 2



করলে ভাগ মিলে গিয়ে 0 ভাগশেষ থাকে। সুতরাং ব্যাপারটা দাঁড়াচ্ছে Fig 2-এর মত। এবার খালি 1000-কে 7 দিয়ে ভাগ করার পালা--

```
7)1000(142
  7
  ---
   30
   28
   ---
    20
    14
    ---
     6
```

ভাগশেষ পাওয়া যাচ্ছে 6. সুতরাং সে কিছু মাত্র গা না ঘামিয়ে (খালি মাথা খাটিয়ে) নাচতে নাচতে গিয়ে আর্কিমিডিসকে বলে দিল যে, গোণা ছয় নম্বর থামে শেষ হয়েছে। ওদিকে বোকা চাকরটা তো গুণেই চলেছে! ■

চালাক চাকরটা যা করল, এটাই হল abstract জিনিস নিয়ে কাজ করা বা abstraction. থামগুলো ছিল ধরাছোঁয়ার জিনিস, কিন্তু তার জায়গায় বসিয়ে দেওয়া হল $1, 2, ..., 6, 0$ সংখ্যাগুলো। ফলে ফিরে ফিরে গোণার কাজটা পরিণত হল ভাগশেষ বার করাতে, যেটা অনায়াসে মনে মনেই সেরে ফেলা যায়। এরকম আরেকটা উদাহরণ দেখা যাক।

Fig 3-এ দ্যাখো একটা সৈনিক দাঁড়িয়ে আছে উত্তর দিকে মুখ করে। বোঝানোর সুবিধার জন্য ওর পায়ের তলায় একটা দিকনির্দেশক কম্পাস এঁকে দিয়েছি। ওকে যদি হুকুম করা হয় "বাঁয়ে মুড়" অমনি ও বাঁদিকে $90°$ মোড় ঘুরে যাবে Fig 4-এর মত, পশ্চিমদিকে মুখ করে। যদি এই অবস্থায় ফের বল "বাঁয়ে মুড়" তবে ও আরো $90°$ মোড় ফিরে Fig 5-র মত করে দক্ষিণ দিকে ফিরে দাঁড়াবে। অবশ্য যদি Fig 3-এই তুমি একবারে "পিছে মুড়" বলতে তবেও ও পিছন ফিরে Fig 5-এর মত দক্ষিণ দিকে মুখ করে দাঁড়াত। একইভাবে Fig 3 থেকে তুমি "ডাইনে মুড়" বললে ও ডানদিকে $90°$ ঘুরবে (Fig 6), মানে পূর্ব দিকে মুখ করবে। অবশ্য তুমি ওকে "হল্ট"-ও বলতে পারো, তবে ও সেই মুহূর্তে যেদিকে মুখ করে আছে, সেভাবেই নট নড়নচড়ন হয়ে দাঁড়িয়ে থাকবে, পরবর্তী হুকুমের অপেক্ষায়।

লক্ষ করো যে, প্রতিটা হুকুম আসলে একটা function. যেমন "বাঁয় মুড়" বললে উত্তরে থাকলে পশ্চিমে, পশ্চিমে থাকলে দক্ষিণে, দক্ষিণে থাকলে পূর্বে, এবং পূর্বে থাকলে উত্তরে মুখ ফেরাবে। অর্থাৎ, "বাঁয় মুড়" হল $\{N, S, E, W\}$ থেকে $\{N, S, E, W\}$-এ এই function-টা--

$$N \mapsto W, \quad W \mapsto S, \quad S \mapsto E, \quad E \mapsto N.$$

Exercise 1: একইভাবে "ডাইনে মুড়", "পিছে মুড়" আর "হল্ট"-এর জন্য function-গুলো কী কী হবে লিখে ফ্যালো। ■

Example 2: এবার ধরো ওকে হুকুম করা হল--

Fig 3

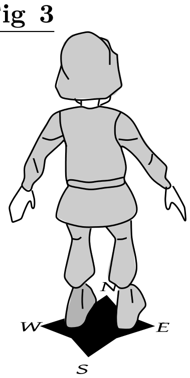


Fig 4

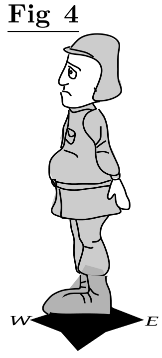


Fig 5

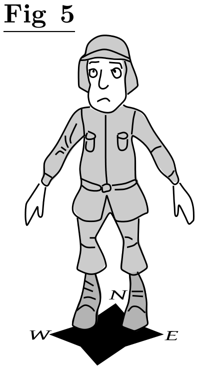
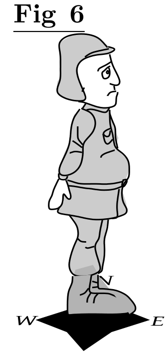


Fig 6



> প্রথমে "বাঁয়ে মুড়, পিছে মুড়", "বাঁয়ে মুড়, পিছে মুড়", এইভাবে 11 বার, তার পর তিন বার "ডাইনে মুড়" বলা হল, সবশেষে বলা হল "হল্ট",

অর্থাৎ মোট হুকুমটা হল

$$\underbrace{\underbrace{\text{বাঁয়ে, পিছে}},\ldots,\underbrace{\text{বাঁয়ে, পিছে}}}_{11 \text{ বার}}, \text{ডাইনে, ডাইনে, ডাইনে, হল্ট!}$$

প্রশ্ন হল সব মিলিয়ে সৈনিকের মুখটা কোন দিকে কতটা ঘুরবে? (যদি অবশ্য ইতিমধ্যেই মাথা ঘুরে পড়ে গিয়ে না থাকে!)
SOLUTION: উত্তরটা বার করার একটা কায়দা হল সেপাইয়ের ভূমিকাটা নিজেই পালন করা। এই পথে মাথা ঘামাতে হয় না, যদিও গা ঘেমে যাওয়ার সম্ভাবনা আছে। গা না ঘামিয়ে খালি মাথা ঘামিয়ে সমাধান করার একটা abstract পদ্ধতি এইরকম--এখানে চার রকম হুকুম আছে-- হল্ট, বাঁয়, পিছে আর ডাইনে।
লক্ষ কর যে, একবার "বাঁয় মুড়" বললে সৈনিকটা 1 ধাপ ঘোরে (ঘড়ির কাঁটার উল্টো দিকে)। দুইবার "বাঁয়" বললে ঘোরে 2 ধাপ, এবং সেটা "পিছে মুড়"-এর সমান। একইভাবে পরপর তিনটে "বাঁয় মুড়" হল 3 ধাপ ঘোরা, যেটা বস্তুতঃ একটা "ডাইনে মুড়"-এর সমান। আর চারবার "বাঁয় মুড়" করলে কী 4 ধাপ ঘুরবে? হ্যাঁ, কিন্তু যেহেতু প্রতি ধাপে 90° করে ঘুরছে, ফলে 4 ধাপ ঘোরা আর 0 ধাপ ঘোরা একই কথা, কারণ দুইক্ষেত্রেই সৈনিকটা ফের গোড়ার অবস্থানে ফিরে আসে (মানে "হল্ট"-এর সমান হয়ে যায়)। আবার 5 বার "বাঁয়" বললে ফের সেটা 1 ধাপ ঘোরার সমান হয়ে যায়। সুতরাং এই হুকুমগুলোর বদলে আমরা $0, 1, 2, 3$ সংখ্যা কল্পনা করতে পারি--

হুকুম	সংখ্যা
হল্ট	0
বাঁয়ে	1
পিছে	2
ডাইনে	3

পরপর দুটো হুকুম মানে যেন হুকুমের সংখ্যা দুটোকে যোগ করে 4 দিয়ে ভাগ করে ভাগশেষ নেওয়া। যেমন পরপর দুবার "ডাইনে" বললে $3 + 3 = 6$, হবে, আর সেটাকে 4 দিয়ে ভাগ করলে ভাগশেষ হবে 2, মানে "পিছে"। লক্ষ কর যে, সত্যিই পরপর দুবার 'ডাইনে" বললে "পিছে"-ই বোঝায়!
সুতরাং আমাদের হুকুমটাকে abstract সংখ্যায় পরিণত করলে হয়

$$\underbrace{(1+2)+\cdots+(1+2)}_{11 \text{ বার}}+3+3+3+0 = 11\times(1+2)+9 = 42,$$

যাকে 4 দিয়ে ভাগ করলে ভাগশেষ থাকে 2, অর্থাৎ "পিছে", অর্থাৎ ও শুরুতে যে দিকে মুখ করে ছিল, পুরো হুকুমটার শেষে ও তার উল্টো দিকে মুখ করে শেষ করবে। যদি ও গোড়ায় Fig 3-এর মত মুখ করে থাকে, তবে শেষ পর্যন্ত দাঁড়াবে Fig 5-এর মত করে। ■

Fig 7

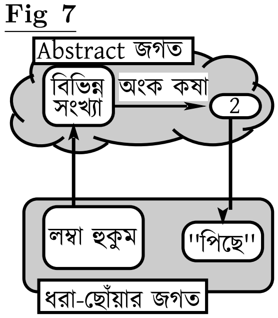


Fig 7 দেখলে বুঝবে abstraction বলতে কী বোঝায়। আমরা ছিলাম ধরা-ছোঁয়ার জগতে। সেখান থেকে উঠে গেলাম abstract জগতে। ধরা-ছোঁয়ার জগতে যেটা ছিল একটা লম্বা হুকুম, সেটা abstract জগতে হয়ে গেল কয়েকটা সংখ্যা। তাদের নিয়ে খানিকটা অংক কষে উত্তর পেলাম 2. অবশেষে এই উত্তরটা নিয়ে আবার নেমে এলাম ধরা-ছোঁয়ার রাজ্যে। এই ব্যাপারটা বস্তুতঃ অংকের সর্বত্রই আছে। কিন্তু abstract algebra-তে এত বেশী রকম আছে যে, প্রায় ম্যাজিকের মত লাগে। যারা অংকের মধ্যে ম্যাজিক দেখতে ভালোবাসো, তাদের পক্ষে এ একেবারে স্বর্গরাজ্য। নীচের অংকটা এরকম একটা উদাহরণ, যেটা abstraction না লাগালে কষা প্রায় অসম্ভব।

Example 3: Fig 8-এ পাঁচটা কাপ রয়েছে, কয়েকটা সোজা আর কয়েকটা উপুড় করা। তোমার কাজ হল কাপগুলোকে

Fig 9-এর মত অবস্থায় নিয়ে আসা। কাজটা করতে হবে ঠিক 10 ধাপে। প্রতি ধাপে তুমি যে কোনো একটা কাপ নিয়ে উল্টে দেবে (মানে সোজা থাকলে উপুড় করে দেবে, আর উপুড় থাকলে সোজা)। কী করে করবে?

SOLUTION: প্রথমে খানিকক্ষণ নিজে চেষ্টা করে দ্যাখো। কাপ না থাকলে কাগজের টুকরো ব্যবহার করতে পারো। কিছুক্ষণ লড়াই করলেই বুঝবে যে, কাজটা ঠিক সহজ নয়। এতরকমভাবে এগোনো যায় যে মাথা গুলিয়ে যায়। যদি খালি 5 ধাপে করতে বলত তবে সহজ ছিল। কাপগুলোকে এক এক করে উল্টে গেলেই চলত। কিন্তু 10 ধাপ অব্ধি চালাতে গেলে কয়েকটা কাপকে একাধিক বার ওল্টাতে হবে। এবং তাতেই সমস্যাটা হবে। ঠিক 10 ধাপের মাথায় Fig 9-এ পৌঁছনো মোটেই সহজ কথা নয়।

এবার abstraction কাজে লাগাই। কাপগুলোর কথা ভুলে যাও। খালি মনে রাখো কতগুলো কাপ এই মুহূর্তে সোজা আছে, সেই সংখ্যাটা even (জোড়) নাকি odd (বিজোড়)। প্রথমে তিনটে কাপ সোজা ছিল, তার মানে odd. প্রথম ধাপে তুমি যাই কর না কেন--

- হয় 4-টে কাপ সোজা হবে, (যদি কোনো উপুড়কে সোজা কর),
- আর নয় তো 2-টো কাপ সোজা থাকবে, (যদি কোনো সোজাকে উপুড় কর)।

সুতরাং প্রথম ধাপের পর সংখ্যাটা even হতে বাধ্য। তারপরের ধাপে ফের odd হতে বাধ্য। এইভাবে odd, even, odd , even করে চলতে চলতে 10 ধাপের পর অবশ্যই odd হতে বাধ্য। কিন্তু Fig 9-তে সোজা কাপের সংখ্যা even. সুতরাং কাজটা করা আসলে অসম্ভব! ■

Abstraction-এর সুবিধা তো দেখলে। কিন্তু অসুবিধাটা হল--কী করে বুঝব যে, ঠিক কোন জিনিসটার কথা ভুলে যাব, আর কোনটাকে হিসেবে রাখব? থামের অংকটাতে যে থামগুলো গুরুত্বপূর্ণ কিছু নয়, সেটা বোঝা কঠিন ছিল না, কিংবা সৈনিকের উদাহরণেও একটু ভাবলেই 4 দিয়ে ভাগ করার ব্যাপারটা মাথায় আসে। কিন্তু কাপের অংকটার বেলায় even, odd-এর ব্যাপারটা মাথায় আসা মোটেই সোজা ছিল না। একটা অংক দেখে চট্ করে কোন অংশটা দরকারী আর কোনটা নিছক গল্প--সেটা বুঝতে পারাটা খুবই প্রয়োজনীয় একটা গুণ। এবং সেইটা শেখাই হল এই বইতে আমাদের প্রধান উদ্দেশ্য। কী করে সেই কাজটা করব সেটা বোঝার জন্য একটা জিনিস লক্ষ কর। এই যে তিনটে উদাহরণ নিলাম, এরা দেখতে সম্পূর্ণ আলাদা--থাম গোণার সঙ্গে সৈনিকের প্যারেড কিংবা কাপ ওল্টানোর আপাতদৃষ্টিতে কোনোই সম্পর্ক নেই। অথচ abstraction করার ফলে কিন্তু তিনটেই মোটামুটি একই জিনিসে পরিণত হল--ভাগ করে ভাগশেষ নেওয়া--

- থামের বেলায় ভাগ করেছিলাম 7 দিয়ে,
- সৈনিকের বেলায় 4 দিয়ে,
- এবং কাপ ওল্টানোর অংকে 2 দিয়ে (odd, even মানে 2 দিয়ে ভাগ করে দেখা ভাগশেষ 1 হয় নাকি 0).

Fig 8



Fig 9



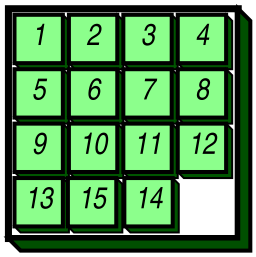


Fig 10

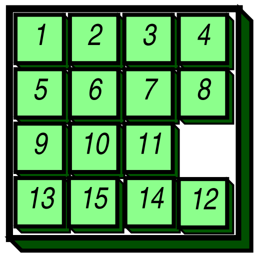


Fig 11

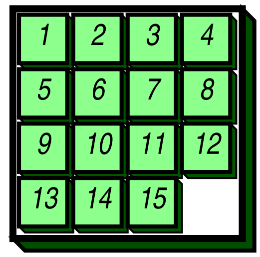


Fig 12

এই ব্যাপারটা অংকের জগতে বার বার দেখা যায়--আপাতদৃষ্টিতে সম্পূর্ণ ভিন্ন সমস্যার মধ্যে একই মূল কাঠামো লুকিয়ে থাকে। ফলে একই কাঠামো বিভিন্ন জায়গায় বার বার ফিরে ফিরে উঁকি দেয়। (যেমন ভাগ নিয়ে ভাগশেষ বার করার ব্যাপারটা)। এইরকম বহুল প্রচলিত কাঠামোগুলোকে যদি abstract-ভাবে চিনে রাখি, তবে ভবিষ্যতে কোনো অংকের মধ্যে লুকিয়ে থাকলেও অমনি চট্ করে ওদের খুঁজে পাব। কাঠামোকে ইংরাজীতে বলে structure. তাই abstract algebra-র মূল উপজীব্য বিষয় হল বিভিন্ন abstract structure নিয়ে আলোচনা করা।
কোনো সমস্যার পিছনে একবার একটা পরিচিত abstract structure-এর হদিস পেয়ে গেলে যে সমস্যাটা কেমন ম্যাজিকের মত সহজ হয়ে যায় তার একটা উদাহরণ এখানে না বললেই নয়।
Fig 10-এ একটা ধাঁধা দেওয়া আছে, যেটা তোমরা ছোটোবেলায় অনেকেই নিশ্চয়ই খেলেছো। একটা ফ্রেমের মধ্যে 15-টা চৌকো টুকরো আছে, তাদের গায় 1 থেকে 15 অব্ধি সংখ্যা লেখা। আর একটা ঘর খালি ফাঁকা আছে। আঙুল দিয়ে টুকরোগুলোকে সরিয়ে সরিয়ে ফাঁকা ঘরে আনা যায়। যেমন Fig 11-এ বারো নম্বর টুকরোটাকে নামিয়ে আনা হয়েছে। ধাঁধাটায় কোনো একটা প্যাটার্ণ দেওয়া থাকে, কাজ হল টুকরোগুলোকে সরিয়ে সরিয়ে সেই প্যাটার্ণে পৌঁছনো। Sam Loyd (স্যাম লয়েড) নামে এক ভদ্রলোক ধাঁধা তৈরীর জন্য বিখ্যাত ছিলেন। তিনি এই ধাঁধাটাকে খুব জনপ্রিয় করেন এইভাবে--

> বিক্রীর সময়ে প্যাটার্ণটা থাকত Fig 10-এর মত। সেখান থেকে পৌঁছতে হবে Fig 12-এ। যে প্রথম করতে পারবে তার জন্য পুরস্কার ঘোষণা করেছিলেন এক হাজার ডলার! 1880 সালে তার মূল্য বড় কম ছিল না।

একে ধাঁধার মজা, তায় টাকার লোভ, দেখতে দেখতে ছেলে মেয়ে বাচ্চা বুড়ো সবাই মিলে স্যাম লয়েডের ধাঁধা কিনে সমাধান করবার জন্য বেজায় খেপে উঠল। এদের মধ্যে অনেকেই দাবী করল যে, তারা একটা সমাধান পেয়েও গেছে। কিন্তু স্যাম লয়েডের সামনে করে দেখাতে গিয়ে সবার সমাধানেই কিছু না কিছু ভুল বেরোতে লাগল। ফলে দেখা গেল যে, পুরস্কার পাওয়া আর কারো কপালেই ঘটছে না। এমন সময়ে একজনের মাথায় abstraction-এর বুদ্ধি খুলল। এবং সেই কায়দাটা লাগাতেই--কিন্তু না, সে কথা এখনই ফাঁস করব না। তৃতীয় অধ্যায়ে গিয়ে যথাসময়ে বলব।
আমরা এই বইতে তিনটে প্রধান abstract structure-এর কথা শিখব--group, ring এবং field. এক্ষুণি যে তিনটে অংক দেখলাম তাদের তিনজনের পিছনেই যে ভাগশেষ করার ব্যাপারটা ছিল সেটা হল group-এর উদাহরণ। স্যাম লয়েডের ধাঁধাটার (যার ইংরাজী নাম হল 15 puzzle) তারও পিছনে আছে একটা group. কিন্তু এদের গভীরে ঢোকার আগে কয়েকটা ধারণার সঙ্গে পরিচিত হতে হবে, যারা যে কোনো abstract structure-এরই মূল উপাদান।

10.1 Abstract structure তৈরীর মাল মশলা

যে কোনো abstract structure-এর পিছনেই প্রথম উপাদান হল একটা set. থামের উদাহরণে আমরা থামগুলোকে নাম দিয়েছিলাম $1, 2, 3, 4, 5, 6$ এবং 0. থামগুলো গুরুত্বপূর্ণ ছিল না, গুরুত্বপূর্ণ ছিল এই set-টা $\{0, 1, 2, 3, 4, 5, 6\}$. সৈনিকের উদাহরণে গুরুত্বপূর্ণ ছিল হুকুমগুলোর set-টা--{হল্ট, বাঁয়ে, পিছে, ডাইনে}. আমরা অবশ্য এটাকে $\{0, 1, 2, 3\}$ বলেও ভাবতে পারি। কাপের উদাহরণে set-টা ছিল {even,odd}.
উদাহরণ তিনটে দেখলেই বুঝবে যে, আমরা set-এর একটা element-এ থেমে থাকছি না। থামের উদাহরণে গোণা যত এগোচ্ছে ততই $1, 2, \ldots$ করে এগোচ্ছে, এবং 6-এর পর ফের 0-তে ফিরে আসছে। কাপের ধাঁধাটাতেও প্রতি ধাপে even থেকে odd, বা odd থেকে even হচ্ছে। এই ব্যাপারটা সবচেয়ে সুন্দরভাবে বোঝা যাবে সৈনিকের উদাহরণে। বিভিন্ন হুকুম মিলে নতুন হুকুম তৈরী হচ্ছে। যেমন পরপর দুবার "বাঁয়" মিলে হল "পিছে"। মনে রেখো যে, হুকুমগুলো সবাই $\{N, S, E, W\}$ থেকে $\{N, S, E, W\}$-এ একেকটা function. আমরা যখন দুটো হুকুমকে মিলিয়ে নতুন হুকুম তৈরী করছি, সেটা আসলে function-এর composition. যেমন--

বাঁয় $\circ$ বাঁয় $=$ পিছে।

এটা যদি স্পষ্ট না হয়ে থাকে, তবে এইভাবে ভাবো--যদি উত্তর দিকে মুখ করে শুরু করে থাকি, তবে প্রথম বার "বাঁয়"-এর পর মুখ থাকবে পশ্চিমে, মানে বাঁয়$(N) = W$. আবার "বাঁয়" লাগালে মুখ ঘুরবে দক্ষিণে, মানে বাঁয়(বাঁয়(N)) $=$ বাঁয়$(W) = S$. আবার পিছে$(N) = S$. শুরুতে যে দিকেই মুখ থাকুক না কেন, একইরকম যুক্তি খাটবে। অর্থাৎ

$\forall x \in \{N, S, E, W\}$ বাঁয়(বাঁয়(x)) $=$ পিছে(x).

একইভাবে প্রথমে "ডাইনে" বলে তারপর "পিছে" বললে সব মিলিয়ে সৈনিকটা বাঁয় ঘোরে--

পিছনে $\circ$ ডাইনে $=$ বাঁয়ে।

অর্থাৎ, in general--

দ্বিতীয় হুকুম $\circ$ প্রথম হুকুম $=$ দুটো মিলিয়ে কী হুকুম দাঁড়ালো।

লক্ষ কর যে $\circ$ দিয়ে আমরা হুকুমের set-টার দুটো element-কে মিলিয়ে আরেকটা element তৈরী করলাম। এই কাজটাকে বলব একটা **binary operation.**

Exercise 2: বল দেখি হল্ট $\circ$ বাঁয় $=$ **?** ■

যদি set-টা ছোটো কিছু হয়, তবে তার উপর একটা binary operation-কে সম্পূর্ণ নামতার মত করে লিখে ফেলা যায়।

Example 4: সৈনিকের উদাহরণে নামতার টেবিলটা লিখে ফ্যালো।

SOLUTION:

		দ্বিতীয় হুকুম			
প্রথম হুকুম	$\circ$	হল্ট	বাঁয়	পিছে	ডাইনে
	হল্ট	হল্ট	বাঁয়	পিছে	ডাইনে
	বাঁয়	বাঁয়	পিছে	ডাইনে	হল্ট
	পিছে	পিছে	ডাইনে	হল্ট	বাঁয়
	ডাইনে	ডাইনে	হল্ট	বাঁয়	পিছে

■

Binary operation ব্যাপারটা অবশ্য আমাদের পক্ষে নতুন কিছু নয়। ছোটো বেলায় আমরা যে যোগ, বিয়োগ শিখি সেসবই binary operation-এর উদাহরণ। যেমন "$2+3=5$" মানে "2 আর 3-কে '+' নামক binary operation দিয়ে মেলালে পাই 5."

Abstract structure-দের বেলায় অনেক সময়ে নতুন নতুন binary operation নিয়ে কাজ করতে হয়। Set-টাকে একটু কায়দা করে লিখলে এই নতুন binary operation-গুলোকে যোগ, বিয়োগ ইত্যাদি পরিচিত binary operation দিয়ে প্রকাশ করা যায়। তাতে লিখতে একটু সুবিধা হয়। যেমন সৈনিকের উদাহরণের set-টাকে যদি $\{0, 1, 2, 3\}$ রূপে লিখি (অর্থাৎ হল্ট $= 0$, বাঁয় $= 1$, ইত্যাদি), তবে দুটো হুকুম মেলানো মানে হল সংখ্যা দুটোকে যোগ করে 4 দিয়ে ভাগশেষ নেওয়া। অনেক সময়ে এরকম binary operation বোঝাতে আমরা নতুন চিহ্নের অবতারণা করি, যেমন আমরা "যোগ করে 4 দিয়ে ভাগশেষ নেওয়া"-কে যদি $\star$ দিয়ে লিখি, তবে--

$$3 \star 2 = 1.$$

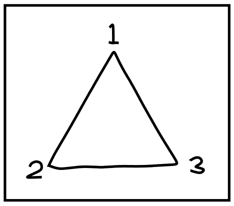


Fig 13

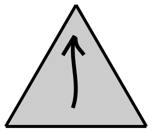


Fig 14

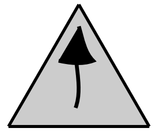


Fig 15

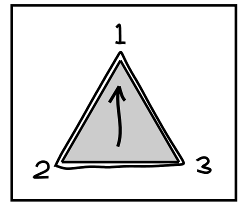


Fig 16

লক্ষ কর যে আমরা যে কোনো $i, j \in \{0, 1, 2, 3\}$-এর জন্যই $i \star j$ বার করতে পারি এইভাবে-- প্রথমে $i + j$ বার কর, তাকে 4 দিয়ে ভাগ করলে যে ভাগশেষ পাবে সেটাই হল $i \star j$.
একইভাবে থামের অংকে binary operation-টা হল যোগ করে 7 দিয়ে ভাগশেষ নেওয়া।
এবার সংজ্ঞাটা গুছিয়ে লিখে রাখি--

DEFINITION: **Binary operation**

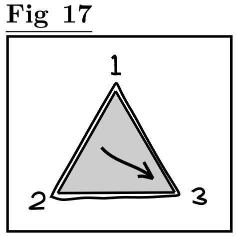
Let S be any nonempty set. By a **binary operation** on S we mean any function

$$f : S \times S \to S.$$

If $s, t \in S$ we often write $f(s, t)$ as $s \star t$ or $s \circ t$ or $s \bullet t$ etc.

Abstraction ব্যাপারটা খুব কাজের বটে, কিন্তু প্রথম প্রথম শেখার সময়ে ধরা-ছোঁয়ার জগতের সঙ্গে যোগসূত্র না রাখলে মাথা গুলিয়ে যাওয়ার সম্ভাবনা। এবার যে উদাহরণটা দেব সেটা এই যোগসূত্র রক্ষা করার জন্যই। এখানে তোমাকে হাতেকলমে কিছু করতে হবে, এবং নিতান্ত অসুবিধা না হলে এই কাজটুকু যেন বাদ দিয়ে যেও না। এই উদাহরণটা group theory শেখার জন্য অত্যন্ত গুরুত্বপূর্ণ, এবং পরবর্তী অধ্যায়গুলোতেও কাজে দেবে।
প্রথমে কাগজ কেটে একটা সমবাহু ত্রিভুজ বানিয়ে নাও, আর খাতার পাতায় একই মাপে একটা ত্রিভুজ এঁকে নাও। এটাকে বলব ফ্রেম (Fig 13)। এর তিন প্রান্তে $1, 2, 3$ লিখে নাও। কাগজের ত্রিভুজটার দুইপিঠের একটাকে বলব "সোজা" আর অন্যটাকে বলব "উল্টো"। দুই পিঠেই একটা করে তীর এঁকে নাও, যেভাবে দেখিয়েছি Fig 14 আর Fig 15-এ। দুটো তীর যেন ঠিক পিঠোপিঠি হয়। লক্ষ করো উল্টো পিঠের তীরটার মাথাটা কালো করে দিয়েছি, যাতে দুটো পিঠকে আলাদা করা যায়।
এবার হাতের ত্রিভুজটাকে এই ফ্রেমের ওপর ফিট্ করে বসিয়ে দাও Fig 16-এর মত করে, যাতে সোজা পিঠটা উপরে থাকে আর তীরটা থাকে ফ্রেমের 1-এর দিকে মুখ করে।
এবার যেটা করব সেটা অনেকটা সৈনিকের উদাহরণের মত। ত্রিভুজটা হল সৈনিক, তীরটা বোঝাচ্ছে সে কোন দিকে মুখ করে আছে, আর ফ্রেমটা হল তার কুচ্কাওয়াজের জায়গা। আমরা সৈনিকটার (মানে ত্রিভুজটার) অবস্থান এমনভাবে পরিবর্তন করব

Fig 17



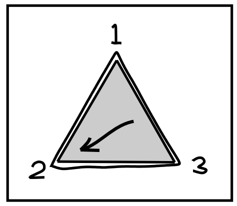


Fig 18



Fig 19

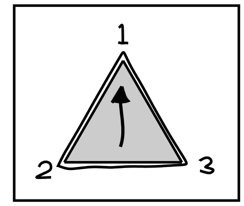


Fig 20

যাতে আবার ফ্রেমে ফিট্ করে যায়। একটা কায়দা হল ডানদিকে একঘর ঘোরানো (যেমন Fig 17-এ)। এই ঘোরানোটার একটা নাম দিই--r. এখানে r যেন $\{1,2,3\}$ থেকে $\{1,2,3\}$-এ একটা function, যেখানে

$$r(1) = 2, \quad r(2) = 3, \quad r(3) = 1.$$

এখানে $r(1) = 2$ মানে হল "ফ্রেমের 1 নম্বরে ত্রিভুজের যে প্রান্তটা ছিল, সেটা চলে গেল ফ্রেমের 2 নম্বরে"। একইভাবে $r(2) = 3$ মানে হল "ফ্রেমের 2 নম্বরে ত্রিভুজের যে প্রান্তটা ছিল, সেটা চলে গেল ফ্রেমের 3 নম্বরে"।
যদি বাঁদিকে একঘর ঘোরাতে, তবে তাকে বলব ℓ, মানে

$$\ell(1) = 3, \quad \ell(2) = 1, \quad \ell(3) = 2.$$

(Fig 18)। সৈনিকের উদাহরণে "হল্ট" মানে ছিল নটনড়নচড়ন হয়ে দাঁড়িয়ে থাকা। ত্রিভুজের ক্ষেত্রে কিছু না করে বসে থাকাকে নাম দেব ধরো e. তার মানে

$$e(1) = 1, \quad e(2) = 2, \quad e(3) = 3.$$

এই পর্যন্ত ব্যাপারটা সৈনিকের উদাহরণের মতই। কিন্তু কাগজের ত্রিভুজের বেলায় আমাদের খানিকটা বেশী স্বাধীনতা আছে, চাইলে আমরা ত্রিভুজটাকে উল্টেও দিতে পারি। (প্যারেড চলাকালীন সৈনিকটাকে তো আর Fig 19-এর মত ডিগবাজি খেতে বলা যায় না!) উল্টে দেওয়াকে যদি f_1 বলি, তবে Fig 16 থেকে শুরু করে f_1 লাগালে পৌঁছব Fig 20-তে। এখানে আমরা ওল্টানো বলতে "ফ্রেমের 1 নম্বর প্রান্তটাকে স্থির রেখে বাঁদিক-ডানদিক ওল্টানো" বোঝাচ্ছি। অতএব f_1 হল এমন একটা function যাতে

$$f_1(1) = 1, \quad f_1(2) = 3, \quad f_1(3) = 2.$$

একইভাবে, যদি ওলটানোর সময়ে ফ্রেমের 2 নম্বর প্রান্তকে স্থির রাখতাম, তবে তাকে নাম দিতাম f_2. যেমন ধরো, Fig 20 থেকে শুরু করে f_2 লাগালে পাবে Fig 18। যদি 3 নম্বর প্রান্তকে স্থির রেখে ওলটাতাম, তবে বলতাম f_3.
একটু চিন্তা করলেই বুঝবে ত্রিভুজটাকে খালি এই 6-ভাবেই ফ্রেমে ফিট্ করা যায়--

$$\{e,\ r,\ \ell,\ f_1,\ f_2,\ f_3\}.$$

সৈনিকের উদাহরণের মতই binary operation-টা এখানেও function composition, যেটাকে সাধারণতঃ $\circ$ চিহ্ন দিয়ে বোঝানো হয়। এখানে পরিশ্রম বাঁচানোর জন্য কোনো চিহ্নই ব্যবহার করব না, মানে $r \circ f_1$ না লিখে স্রেফ rf_1 লিখে ছেড়ে দেব।

Example 5: বল তো এখানে f_2^2 আর $f_3 r$ কী কী হবে?

SOLUTION: f_2^2 মানে তো পরপর দুবার ওল্টানো, 2 নম্বর প্রান্তকে স্থির রেখে। এর ফলে আবার গোড়ার অবস্থায় ফিরে আসব। তাই $f_2^2 = e$.
কিন্তু $f_3 r$ (মানে প্রথমে ঘুরিয়ে তারপর ওল্টানো) ঠিক কী হবে সেটা মনে মনে বার করা অত সোজা নয়। হাতেকলমে করে দ্যাখো, উত্তর পাবে--f_1. ■

Exercise 3: একইভাবে বল $f_1 r^2$ কি হবে। আর $(rf_1r)^2$-ই বা কি হবে? ■

DAY 11
Binary operation-দের বিভিন্ন ধর্ম

অংকের দুনিয়ায় আমাদেরকে নানারকম binary operation নিয়ে কাজ করতে হয়। তাদের মধ্যে কেউ কেউ স্কুল থেকেই আমাদের পরিচিত, কেউ বা নতুন। যদি কোনো মানুষ বিদেশ-বিভুঁইতে যায়, সেখানে যেমন সে কোনো পরিচিত লোকের দেখা পেলে খুশি হয়, বা কোনো পরিচিত পরিবেশের সঙ্গে সাদৃশ্য দেখলে স্বচ্ছন্দ বোধ করে, তেমনি অপরিচিত binary operation-দের নিয়ে কাজ করার সময়ে আমাদেরও সেই দশা হয়। চেনা-জানা binary operation-এর যে সব ধর্ম আমরা ছোটোবেলা থেকেই ব্যবহার করে আসছি, তার কয়েকটাও যদি এই অপরিচিতদের মধ্যে খুঁজে পাই, তবে তাদের নিয়ে অংক করা অনেক সহজ হয়।
একটা উদাহরণ দিই। আমরা ছোটোবেলা থেকেই জানি গুণ করার সময়ে কে আগে কে পরে তাতে কিছু এসে যায় না, যেমন $2 \times 3 = 3 \times 2$. এবার হায়ার সেকণ্ডারীতে উঠে যখন দুটো matrix-কে গুণ করা শিখি, তখনও বারবার অভ্যাসবশতঃ $AB = BA$ লিখে ফেলতে হাত নিশ্‌পিশ্‌ করে। এর কারণ আর কিছুই নয়, পরিচিত জিনিসের প্রতি মানুষের সহজাত আকর্ষণ। যত binary operation আছে, তার মধ্যে সবচেয়ে বেশী পরিচিত হল দুটো integer-কে যোগ করা। অধিকাংশ মানুষের জীবনেই প্রথম অংক কষা শুরু হয় যোগ করা দিয়েই। সেই কারণে যোগের বিভিন্ন ধর্ম আমাদের মজ্জায় মজ্জায় গেঁথে যায়, এবং সেই ধর্মগুলো নতুন কোনো binary operation-এর মধ্যে খুঁজে পেলে আমাদের মন নেচে ওঠে। এইরকম একগুচ্ছ ধর্ম নিয়ে এবার আলোচনা করব।

11.1 Closure

দুটো positive integer-কে যোগ করলে উত্তরটা আবার একটা positive integer-ই হয়, কোনোভাবেই negative বা ভগ্নাংশ-টগ্নাংশ কিছু এসে গিয়ে ঝামেলা বাঁধায় না। বস্তুতঃ সেই কারণেই আমরা বাচ্চাদের যোগ করা দিয়ে অংক শেখানো শুরু করি। যোগের এই ধর্মটা দিয়েই আমাদের আলোচনাও শুরু করা যাক।
আমরা দেখেছি যে, কোনো set S-এর উপরে একটা binary operation মানে হল $S \times S$ থেকে S-এ একটা function. এর মধ্যে দুটো কথা লুকিয়ে আছে--

- S-এর যে কোনো দুজন সদস্যের মধ্যে binary operation-টা করা যাবে,
- এবং এর ফলে যে পদার্থটা পাওয়া যাবে, সেটা ফের S-এর মধ্যেই থাকবে।

এই দুটো শর্তই binary operation-এর সংজ্ঞার মধ্যেই ধরা আছে, সুতরাং নতুন করে আর বলার কিছু নেই, কিন্তু অনেক সময়ে এই দুটো শর্তকে একটা গালভরা নাম দেওয়া হয়--**closure property.** একটা উদাহরণ নেওয়া যাক।
আমাদের set-টা যদি $\mathbb{N}$ হয়, তবে যোগ করা যে একটা binary operation, সে তো বললামই। কিন্তু বিয়োগ করাও কি একটা binary operation? না, কারণ যে কোনো দুটো positive integer দেওয়া থাকলে একটা থেকে অন্যটা বিয়োগ করা যায় বটে, কিন্তু বিয়োগফলটা একটা positive integer নাও হতে পারে, যেমন $2 - 3 = -1$, যেটা মোটেই একটা positive integer নয়। এই কারণেই আমরা বাচ্চাদের অংক শেখানো সময়ে প্রথমেই বিয়োগ শেখাতে যাই না! সুতরাং আমরা বলব যে, $\mathbb{N}$-এর উপরে '$-$' একটা binary operation নয়। এইটাকেই বড় করে লেখা যায়--

'$-$' does not satisfy closure property on $\mathbb{N}$.

কখনো বা লেখা হয়--

$\mathbb{N}$ is not closed under '$-$'।

(সাবধান, এই closed-এর সঙ্গে কিন্তু real analysis-এর closed-এর কোনো সম্পর্ক নেই!)
একইরকম সমস্যার জন্য $\div$-কে $\mathbb{Z}$-এর উপরে একটা binary operation বলতে পারি না, কারণ $1 \div 2 \notin \mathbb{Z}$. আচ্ছা, যদি যাবতীয় rational সংখ্যার set-টা (মানে $\mathbb{Q}$, যার মধ্যে integer-রাও আছে, fraction-রাও আছে) সেটা নিই, তার উপরে কি $\div$ একটা binary operation হবে? দুঃখের বিষয় এখানেও একটা গলদ থেকে গেছে। $0 \in \mathbb{Q}$, কিন্তু 0 দিয়ে কোনো সংখ্যাকে ভাগ করা যায় না। আমরা তাই আবার বলব

$\mathbb{Q}$ is not closed under $\div$.

অবশ্য যদি গুণ করার কথা ভাবি, তবে কিন্তু যে কোনো দুটো $a, b \in \mathbb{Q}$-কে গুণ করলে $a \times b \in \mathbb{Q}$ হয়। তাই বলব যে,

$\mathbb{Q}$ is closed under $\times$.

"Closed হওয়া"-কে এক কথায় বলে "closure." বস্তুতঃ closure ব্যাপারটা binary operation-এর সংজ্ঞার মধ্যেই ধরা আছে। তাই অধিকাংশ standard বইতেই এটা আর আলাদা করে উল্লেখ করে না। কিন্তু আমরা তো সবে সবে শেখা শুরু করছি, তাই এই বইতে closure শর্তটা সব সময়ে আলাদা করে উল্লেখ করব।

Example 6: ধরো M হল যাবতীয় 2×3 matrix-এর set. এই set-টা কি closed under matrix multiplication?

SOLUTION: Closed under matrix multiplication হওয়া মানে M-এর যে কোনো দুজন সদস্যকে matrix multiplication করা যাবে এবং গুণফলটা ফের M-এর মধ্যে থাকবে। একটু চিন্তা করলেই বুঝবে যে প্রথম শর্তটাই এখানে মিলছে না, দুটো 2×3 matrix-কে পরস্পরের সঙ্গে গুণ করাই যায় না, কারণ যদি $A, B \in M$ হয়, তবে AB বার করা অসম্ভব, যেহেতু A-র column-এর সংখ্যা আর B-র row-এর সংখ্যা সমান নয়। সুতরাং এখানে M-টা closed under matrix multiplication হল না। ■

Closure property না থাকলে সেইরকম binary operation নিয়ে আমরা পারতপক্ষে কাজ করি না। এরকম binary operation নিয়ে কাজ করতে যাওয়া যেন রেলিং ছাড়া ছাদে ছুটোছুটি করে খেলতে যাওয়ার মত, কখন যে বেমক্কা ছাদের বাইরে গিয়ে পড়বে কিচ্ছু ঠিক নেই!

Exercise 4: নীচে কয়েকটা binary operation দেওয়া হল। বল তো কোন কোন ক্ষেত্রে $\mathbb{N}$-টা closed under the binary operation হবে--

(1) $a \star b = a \times b$, **(2)** $a \star b = a^b$, **(3)** $a \star b = a^2 - b$, **(4)** $a \star b = a^2b^2 + b - ab$

■

আমরা যখন সৈনিকের উদাহরণটা করছিলাম, তখন একটা হুকুম ছিল 'হল্ট'। এই হুকুমটা হয়তো একটু বোকা বোকা লেগেছিল--কিছু না করার জন্য আবার আলাদা একটা হুকুমের কী দরকার? কিন্তু ওই হুকুমটার প্রয়োজন বুঝবে নীচের অংকটা দেখলেই।

Example 7: আমরা সৈনিকের উদাহরণে binary operation-টা ছিল function composition, যার চিহ্ন '$\circ$' যদি "হল্ট" হুকুমটা বাদ দিতাম তবে খালি { বাঁয়, পিছে, ডাইনে }-এর উপরে কি $\circ$ একটা binary operation হত?

SOLUTION: না, কারণ সেক্ষেত্রে "বাঁয়$\circ$ডাইনে" চলে যেত set-টার বাইরে। ■

Exercise 5: Which of the following sets are closed under matrix multiplication?

1. The set of all 2×2 diagonal matrices.
2. The set of all 2×2 upper triangular matrices.
3. The set of all 2×2 lower triangular matrices.
4. The set of all 2×2 triangular matrices.

HINT:
এই অংকটা তোমার নিজের করবার জন্য। খালি কায়দাটা ধরিয়ে দিতে প্রথমটা করে দিচ্ছি। আগে মনে করিয়ে দিই যে, 2×2 diagonal matrix-রা হল এইরকম--

$$\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix},$$

যেখানে a, b যে কোনো সংখ্যা।
এদের set-টা closed under matrix multiplication হয় কিনা দেখতে হবে, মানে এরকম চেহারার দুটো যে কোনো matrix-কে গুণ করলে গুণফলটা আবার diagonal হয় কিনা। ধরো দুটো diagonal matrix নিলাম--

$$\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \text{ আর } \begin{bmatrix} c & 0 \\ 0 & d \end{bmatrix}.$$

লক্ষ কর আমরা a, b, c, d ইত্যাদি চিহ্ন ব্যবহার করেছি, কোনো সংখ্যা নয়। যাতে যুক্তিটা general থাকে। এবার গুণ করে দিই--

$$\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \begin{bmatrix} c & 0 \\ 0 & d \end{bmatrix} = \begin{bmatrix} ac & 0 \\ 0 & bd \end{bmatrix},$$

যেটা আবার একটা diagonal matrix. সুতরাং বলতে পারি যে, "The set of all 2×2 diagonal matrices is closed under matrix multiplication."
এবার বাকি অংকগুলো নিজে নিজে কর। খালি মনে করিয়ে দিই যে, 2×2 upper triangular matrix-দের চেহারা হল

$$\begin{bmatrix} a & b \\ 0 & c \end{bmatrix},$$

যেখানে a, b, c যে কোনো সংখ্যা।
একইভাবে 2×2 lower triangular matrix-রা হল

$$\begin{bmatrix} a & 0 \\ b & c \end{bmatrix},$$

যেখানে a, b, c যে কোনো সংখ্যা।
যখন খালি triangular matrix-এর set-এর কথা বলা হচ্ছে, তখন তার মধ্যে upper এবং lower triangular দুই ধরণেরই matrix আছে বুঝতে হবে। ■

Exercise 6: মনে কর $\mathbb{Z}$-এর উপরে একটা binary operation দিলাম $a \star b = a + b - ab$. প্রশ্ন করা হল যদি $\mathbb{Z}$-এর জায়গায় $\mathbb{N}$ নিতাম, তবেও কি $\star$ একটা binary operation থাকত? দুজন ছাত্র এই নিয়ে এইভাবে ঝগড়া করছে--

- প্রথম জন বলছে--যদি $20, 30 \in \mathbb{N}$ নিই, তবে

$$20 \star 30 = 20 + 30 - 20 \times 30 = -550,$$

  যেটা $\mathbb{N}$-এর বাইরে চলে যাচ্ছে। সুতরাং $\mathbb{N}$ নিশ্চয়ই closed under $\star$ হতে পারে না।

- দ্বিতীয় জন বলছে--কিন্তু যদি $1, 2 \in \mathbb{N}$ নিই, তবে

$$1 \star 2 = 1 + 2 - 1 \times 2 = 1,$$

  যেটা দিব্যি $\mathbb{N}$-এর মধ্যেই থাকছে। সুতরাং $\mathbb{N}$ নিশ্চয়ই closed under $\star$ হবে।

- সেটা শুনে প্রথম ছাত্র বলছে--তুই তো খালি একটা উদাহরণ নিয়ে দেখালি।

- দ্বিতীয় ছাত্র বলল--তুইও তো ভাই খালি একটাই উদাহরণ নিয়ে দেখালি, তবে আমার বেলাতেই দোষ হল কেন?

এই ঝগড়ার কী করে নিষ্পত্তি করবে? ■

11.2 Commutative

এবার যোগের আরেকটা অতি পরিচিত ধর্ম নিয়ে আলোচনা করি। আমরা জানি যে, a, b যে কোনো দুটো সংখ্যা হলে $a + b = b + a$ হয়। অর্থাৎ a, b-র মধ্যে কোনটাকে আগে লিখছি তাতে উত্তরটা বদলায় না। সৈনিকের উদাহরণটা দ্যাখো। সেখানেও একই ব্যাপার। যদি আগে বাঁদিকে ঘুরে তারপর পিছনে ফেরে, তবেও যা হবে, আগে পিছনে ফিরে পরে বাঁদিকে ঘুরলেও একই ব্যাপার হত। এরকমটা যদি কোনো binary operation-এর ক্ষেত্রে সব সময়েই হয়, তবে তাকে বলে **commutative.** এমন বহু binary operation আছে যারা commutative নয়।

Exercise 7: ধরো $\mathbb{R}$-এর উপর দুটো binary operation দিলাম--গুণ আর বিয়োগ। মানে $a \times b$ এবং $a - b$. এদের মধ্যে ঠিক এক জন commutative নয়। কোন জন? ■

> DEFINITION: **Commutative**
>
> Let S be a nonempty set and $\star$ be a binary operation on S. We call $\star$ **commutative** if
>
> $$\forall s, t \in S \quad s \star t = t \star s.$$

Example 8: ধরো আমরা $\mathbb{N}$-এর উপরে একটা binary operation নিলাম

$$a \star b = a^b.$$

দেখাই যাচ্ছে যে $2 \star 4 = 2^4 = 16 = 4^2 = 4 \star 2$. তার মানে কি $\star$-টা commutative?
SOLUTION: না, যদি সব $a, b \in \mathbb{N}$-এর জন্য $a \star b = b \star a$ হত, একমাত্র তবেই commutative বলতাম। এখানে $2^3 \neq 3^2$. ■

Exercise 8: এই অংকটা সেই ত্রিভুজ নিয়ে। মনে আছে আশা করি যে, r মানে ছিল এক ঘর ডানদিকে ঘোরানো, আর f_1 মানে ছিল ওল্টানো (ফ্রেমের 1-এ যে প্রান্তটা আছে, সেটাকে স্থির রেখে)। এবার বল তো $rf_1 = f_1 r$ হবে কি? rf_1 মানে আগে উল্টে পরে ঘোরানো, এবং $f_1 r$ মানে আগে ঘুরিয়ে পরে ওল্টানো।
HINT: হাতেকলমে কাজ দুটো করে দ্যাখো, তাহলেই বুঝবে। ■

11.3 Identity

আবার আমরা ছোটোবেলায় ফিরে যাই। এবার আমরা integer-দের যোগ করার আরেকটা অতি পরিচিত ধর্ম নিয়ে আলোচনা করব। যদি কোনো সংখ্যার সঙ্গে 0 যোগ করি তবে সংখ্যাটা বদলায় না, অর্থাৎ

$$\forall n \in \mathbb{Z} \quad 0 + n = n + 0 = n.$$

এই কথাটা আমরা স্কুল থেকেই জানি। তবে এখন কিনা আমরা অনেক বড় হয়ে গিয়েছি, তাই বেশ গালভরা ভাষায় গম্ভীর মুখে বলব-- $\mathbb{Z}$-এর মধ্যে $+$-এর **identity element** হল 0.
একইভাবে, গুণের ক্ষেত্রে যদি 1 দিয়ে গুণ করি, তবে সংখ্যাটা বদলাবে না, মানে

$$\forall n \in \mathbb{Z} \quad 1 \times n = n \times 1 = n.$$

সুতরাং বলতে পারি যে, $\mathbb{Z}$-এর মধ্যে গুণের identity element হল 1.

DEFINITION: Identity

Let S be any set and let $\star$ be any binary operation defined on it. Then an element $e \in S$ is called an **identity** for $\star$ in S if

$$\forall s \in S \quad e \star s = s \star e = s.$$

Example 9: সৈনিকের উদাহরণে "হল্ট" ছিল identity element, কারণ ওই হুকুমটাতে সৈনিকের অভিমুখের কোনো পরিবর্তন হয় না। ■

যে কোনো binary operation-এর জন্যই যে identity element থাকবেই এমন কোনো কথা নেই। যেমন নীচের উদাহরণে।

Example 10: ধরো $2\mathbb{Z}$ হল যাবতীয় even (জোড়) সংখ্যার set. তাহলে যদি যে কোনো দুটো সংখ্যা $a, b \in 2\mathbb{Z}$ নিই, $a \times b$-ও ফের $2\mathbb{Z}$-এর মধ্যেই থাকবে। তাই '$\times$' হল $2\mathbb{Z}$-এর উপরে একটা binary operation. এর কি কোনো identity element আছে?

SOLUTION: না, কারণ যদি $e \in 2\mathbb{Z}$ একটা identity element হত, তবে আমাদের দরকার হচ্ছে

$$\forall n \in \mathbb{Z} \quad e \times n = n \times e = n.$$

যদি $n = 2$ নিই, তবে $2e = 2$ চাই, তাই $e = 1$ হওয়া ছাড়া পথ নেই। কিন্তু $1 \notin 2\mathbb{Z}$. ■

লক্ষ কর যে, identity element-এর সংজ্ঞার মধ্যে দুটো শর্ত রয়েছে-- $e \star s = s$ এবং $s \star e = s$. যদি $\star$-টা commutative হয়, তবে এর যে কোনো একটা চাপালেই চলত, অন্যটা আপনা আপনিই হত। কিন্তু যদি commutative না হয়, তবে অনেক সময়ে দেখা যায় যে, এই দুটো শর্তের মধ্যে একটা পালিত হচ্ছে, কিন্তু অন্যটা হচ্ছে না। এরকম ক্ষেত্রে আমরা identity না বলে **left identity** বা **right identity** বলি। সংজ্ঞাটা এইরকম--

DEFINITION: Left and right identities

Let S be any set and let $\star$ be any binary operation defined on it. Then an element $e_1 \in S$ is called a **left identity** for $\star$ in S if

$$\forall s \in S \quad e_1 \star s = s.$$

Similarly, an element $e_2 \in S$ is called a **right identity** for $\star$ in S if

$$\forall s \in S \quad s \star e_2 = s.$$

একটা উদাহরণ রয়েছে নীচের অংকটায়।

Example 11: Prove that in the groupoid $(\mathbb{Z}, -)$, there is no left identity, but 0 is a right identity.[2] **(2010.3aii)**

SOLUTION: এখানে groupoid বলে একটা শব্দ ব্যবহার করা হয়েছে। এর মানে হল একটা nonempty set এবং তার উপর যে কোনো একটা binary operation. এই দুটো জিনিসকে একত্রে বলে একটা groupoid. এটা খুব বহুলপ্রচলিত term নয়। আমাদের অংকে groupoid-টা হল $(\mathbb{Z}, -)$. তার মানে set-টা হল $\mathbb{Z}$ এবং binary operation-টা হল '$-$'। সব সময়ে এইভাবে লেখাই নিয়ম, ফার্স্ট ব্র্যাকেটের মধ্যে প্রথমে set-টা, এবং তারপর কমা দিয়ে binary operation-টা।

First part: Let, if possible, the groupoid have a left identity $n \in \mathbb{Z}$.
Then $\forall a \in \mathbb{Z}$ $n - a = a$,
$\therefore$ Putting $a = 1$ we have $n - 1 = 1$.
So $n = 2$.
Again, putting $a = 2$ we should have $n - 2 = 2$.
But $n - 2 = 2 - 2 = 0 \neq 2 (\Rightarrow\Leftarrow)$.
Second part: We know that

$$\forall a \in \mathbb{Z} \quad a - 0 = a.$$

So 0 is a right identity.

■

এক আকাশে যেমন দুই সূর্য শোভা পায় না, তেমনি একটা binary operation-এর কখনও একাধিক identity থাকতে পারে না। একটাও identity নেই, এমনটা হতেই পারে, কিন্তু দুটো আলাদা আলাদা identity আছে এমনটা অসম্ভব। এটাই নীচের theorem-টার বক্তব্য।

THEOREM

Let S be any nonempty set with a binary operation $\star$. If $e_1, e_2 \in S$ are both identity elements for $\star$, ie,

$$\forall s \in S \qquad e_1 \star s = s \star e_1 = s$$
$$\forall s \in S \qquad e_2 \star s = s \star e_2 = s.$$

Then we must have $e_1 = e_2$.

Proof:

We have

$$\forall s \in S \quad e_1 \star s = s.$$

In particular, putting $s = e_2$ we have $e_1 \star e_2 = e_2$.

Again, we have

$$\forall s \in S \quad s \star e_2 = s.$$

So putting $s = e_1$, we get $e_1 \star e_2 = e_1$.

So $e_1 = e_1 \star e_2 = e_2$, as required.

[Q.E.D]

এই প্রমাণটা ভালো করে লক্ষ করো। তারপর একই কায়দায় নীচের অংকটা কর।

Exercise 9: Let S be any nonempty set with a binary operation $\star$. If $e_1 \in S$ is a left identity and $e_2 \in S$ is a right identity, then show that

$$e_1 = e_2 = \text{ identity.}$$

■

এবারের অংকটা খুবই সোজা, কিন্তু একটু ঠকানো।

Exercise 10: ধরো set-টা নিলাম $\mathbb{Z} \times \mathbb{Z}$, মানে element-গুলো হল (m, n)-এর মত, যেখানে $m, n \in \mathbb{Z}$. এর উপর একটা binary operation এইরকম--

$$(m, n) \star (p, q) = (mp, nq),$$

অর্থাৎ প্রথম দুটো সংখ্যাকে ধরে গুণ করে দিলাম, আবার পরের দুটোকেও আলাদা করে গুণ করে দিলাম। এইবার বল দেখি--

1. এর কি কোনো identity element আছে?
2. এবার $\mathbb{Z} \times \mathbb{Z}$-এর বদলে তার একটা subset নিই--$2\mathbb{Z} \times \mathbb{Z}$, যার element-গুলো দেখতে $(2m, n)$-এর মত, মানে প্রথম integer-টা even. এবার কি binary operation-টার কোনো identity element আছে?
3. এবার আরও ছোটো একটা subset নেব--$\{0\} \times \mathbb{Z}$, যার element-গুলো দেখতে $(0, n)$-এর মত। Binary operation-টা একই রাখলাম। এবার কি কোনো identity element আছে?

■

11.4 Inverse

আমরা অনেকক্ষণ যোগের বিভিন্ন ধর্ম আলোচনা করছি, কারণ সেটাই আমাদের সবচেয়ে পরিচিত binary operation. কিন্তু ছোটোবেলায় অংক শেখা তো খালি যোগ অংকেই থেমে থাকে না, যোগের পরেই আসে বিয়োগ। একটু ভাবলেই দেখবে '$-$ ' চিহ্নটা আমরা দুইভাবে ব্যবহার করি--

1. দুটো সংখ্যার মাঝখানে, যেমন $3 - 2$. তখন এটা বিয়োগ করা বোঝায়।
2. কোনো সংখ্যার আগে, যেমন -5, তখন একটা negative বোঝায়।

এই দুই ব্যবহারের মধ্যে সাধারণতঃ প্রথমটাই আমরা আগে শিখি। দ্বিতীয়টা শিখি একটু বড় হয়ে। কিন্তু প্রথমটা আসলে আসে দ্বিতীয়টা থেকেই, কারণ

$$a - b = a + (-b).$$

আমরা সাধারণতঃ $-b$-কে বলি "মাইনাস b"। কিন্তু অংকের গালভরা ভাষায় ওকে বলে “inverse of b under addition”, অর্থাৎ সেই সংখ্যা যা b-এর সঙ্গে যোগ করলে 0 পাওয়া যায়।

> DEFINITION: **Inverse**
>
> Let S be any nonempty set and let $\star$ be any binary operation defined on it with identity element e. Let $s \in S$. We call $t \in S$ an **inverse** of s if
>
> $$t \star s = s \star t = e.$$

Example 12: ধরো যাবতীয় positive real number-এর set-টা নিলাম, মানে $(0, \infty)$, আর binary operation-টা নিলাম "গুণ করা", তবে 3-এর inverse কী হবে?
SOLUTION: এখানে identity হল 1. তার মানে 3-এর inverse হল সেই সংখ্যা যার সঙ্গে 3 গুণ করলে 1 হয়। সুতরাং inverse-টা হল $\frac{1}{3}$. ■

Exercise 11: সৈনিকের উদাহরণে "বাঁয়"-এর inverse যে "ডাইনে", সেটা নিশ্চয়ই বলে দিতে হবে না। বলতে পারো "পিছে"-র inverse কি? ■

সব binary operation-এর ক্ষেত্রেই যে inverse থাকবেই এমন কথা নেই। যে সব binary operation-এর জন্য কোনো identity-ই পাওয়া যায় না, তাদের ক্ষেত্রে তো প্রশ্নটা inverse অব্ধি গড়ায়ই না। কিন্তু যাদের বেলায় identity থাকেও, তাদের বেলাতেও অনেক সময়ে সব element-এর inverse থাকে না। যেমন ধরো নীচের উদাহরণটা।

Example 13: আমরা কাজ করব $(\mathbb{N} \cup \{0\}, +)$ নিয়ে, মানে set-টা হল $\{0, 1, 2, ...\}$ আর binary operation-টা হল যোগ করা। বুঝতেই পারছ যে 0 হল identity. এখানে কোন কোন element-এর inverse আছে?
SOLUTION: খালি 0-র inverse আছে, $-0 = 0$, বাকিদের কারুরই inverse নেই, কারণ কোনো negative সংখ্যা আমাদের set-এ নেই। এখানে তুমি binary operation-টা ব্যবহার করে খালি এগোতেই পারো, পিছোবার কোন পথ নেই। ■

যদি b হয় a-র inverse, তবে a আবার হবে b-র inverse. সেটা বোঝাই যায় কারণ "b হল a-র inverse" মানে

$$a \star b = b \star a = e.$$

আর "a হল b-র inverse" মানে

$$b \star a = a \star b = e.$$

দেখতেই পাচ্ছ যে, দুটো জিনিস আসলে একই।

11.5 Associativity

এবার একটা শর্তের কথা শিখব যেটা খুবই কাজের, কিন্তু চট্ করে দেখে যার উপযোগিতা বোঝা যায় না। আমরা যে তিনটে উদাহরণ দিয়ে শুরু করেছিলাম তার সবগুলোতেই মূল কথা ছিল-- অনেকগুলো ধাপ পরপর করে গেলে শেষ পর্যন্ত কী দাঁড়াবে সেটা হিসেব করে বার করে দেওয়া, যেমন থামের উদাহরণে প্রশ্ন ছিল $1, 2, \ldots$ করে 1000 অবধি গুণলে কোণ থামে গোণা শেষ হবে। ধাপগুলোকে পরপর মেলানোর কাজটা হচ্ছে binary operation-টা দিয়ে। যেমন সৈনিকটাকে দুবার পরপর বাঁয়ে ঘুরতে বললে আসলে সেটা পিছনে ফেরা বোঝায়। যেহেতু এটা একটা binary operation, তাই এককে বারে খালি দুটো করে ধাপ মেলানো যাবে। সুতরাং দুয়ের বেশী ধাপ মেলাতে হলে binary operation-টাকে বার বার করে লাগানো ছাড়া পথ নেই। এবং সেই কাজেই আমাদের প্রধান সহায় হল **associativity.** প্রথমে একটা উদাহরণ দিয়ে বুঝে নিই। ছোটোবেলায়

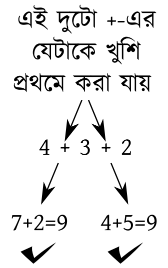


Fig 21

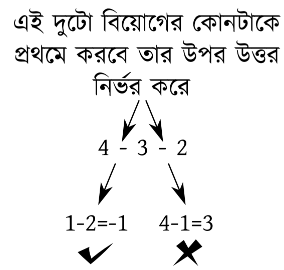


Fig 22

যখন আমরা যোগ বিয়োগ শিখি, তখন এদের মধ্যে একটা গুরুত্বপূর্ণ পার্থক্যও আমাদের শেখানো হয়। ধরো এই দুটো অংক, $4+3+2=?$ আর $4-3-2=?$ প্রথমক্ষেত্রে দুটো যোগের যেটাকে খুশি প্রথমে করতে পারো (Fig 21)। কিন্তু বিয়োগের বেলায় সে স্বাধীনতা নেই (Fig 22)। এই স্বাধীনতার ধর্মটা আছে বলেই আমরা $+$-কে বলি একটা associative binary operator. সংজ্ঞাটা এইরকম--

DEFINITION: Associative

Let S be any nonempty set and let $\star$ be any binary operation defined on it. We call $\star$ **associative** if

$$\forall s,t,u\in S \quad (s\star t)\star u = s\star(t\star u).$$

আমরা অংকে যে সব binary operation নিয়ে কাজ করি, তারা অধিকাংশই associative, যেমন স্কুলে শেখা যোগ বা গুণ। প্রচলিত বিভিন্ন binary operation-এর মধ্যে তিনজন আছে যারা associative নয়। এদের পরিচয় নিয়ে রাখি।

Example 14: বিয়োগ করা $\mathbb{Z}$-এর উপরে associative নয়, সেটা তো Fig 22 থেকেই দেখেছি। Associativity মানুষের কাছে কতটা স্বাভাবিক ব্যাপার, সেটা ভালো করে বোঝা যায় কোনো বাচ্চাকে অংক শেখাতে গেলে। অধিকাংশ বাচ্চাই স্বাভাবিকভাবে "$(4-3)-2=4-(3-2)$ " ভেবে বসে, ওখানে যে "মাইনাসটাকে কমন নিয়ে" $4-(3+2)$ লিখতে হয়, সেটা তাদের মাথায় ঢোকাতে বেশ বেগ পেতে হয়। Abstract algebra করার সময়ে আমরা পারতপক্ষে non-associative কোনো binary operation নিয়ে কাজ করি না। ■

Exercise 12: বিয়োগ করা যেমন associative নয়, তেমনি আন্দাজ করতে পারছ যে, ভাগ করাও associative হতে পারে না। অবশ্য ভাগ করাটা যাতে আদৌ একটা binary operation হয়, তার জন্য 0-টাকে বাদ দিতে হবে। সুতরাং এখানে আমরা set-টা নেব $\mathbb{R}\setminus\{0\}$. একটা উদাহরণ দিয়ে দেখাও যে $\mathbb{R}\setminus\{0\}$-এর উপরে ভাগ করাটা সত্যিই non-associative. ■

Exercise 13: আরেকটা অতি পরিচিত binary operation আছে $\mathbb{N}$-এর উপরে যেটা associative নয়। সেটা কী বলতে পারো? ■

Associative binary operation নিয়ে কাজ করার অনেক সুবিধা। তার মধ্যে অন্যতম বড় সুবিধা এই যে, কোনো element-এর একাধিক inverse থাকতে পারে না। এমন element পাওয়া যেতেই পারে, যার কোনোই inverse নেই, কিন্তু যদি inverse থাকে, তবে ঠিক একটাই থাকবে। এটাই বলা হয়েছে নীচের theorem-টায়।

THEOREM

Let S be any nonempty set, and let $\star$ be any associative binary operation on S with identity element e. Let $a \in S$. If $b_1, b_2 \in S$ are both inverses of a, ie,

$$\begin{aligned} a \star b_1 = b_1 \star a &= e \\ a \star b_2 = b_2 \star a &= e. \end{aligned}$$

Then we must have $b_1 = b_2$.

Proof:

We have

$$\begin{aligned} b_1 &= b_1 \star e \\ &= b_1 \star (a \star b_2) \quad [\because e = a \star b_2] \\ &= (b_1 \star a) \star b_2 \quad [\because \text{associative}] \\ &= e \star b_2 \quad [\because b_1 \star a = e] \\ &= b_2, \end{aligned}$$

as required.

[Q.E.D]

প্রমাণটা খুব ভালো করে লক্ষ কর। আমাদের চারটে তথ্য দেওয়া ছিল--

$$a \star b_1 = e, \quad b_1 \star a = e, \quad a \star b_2 = e \text{ এবং } b_2 \star a = e$$

কিন্তু প্রমাণটা করতে চারটেই লেগেছে কি? এই কথাটা মাথায় রেখে নীচের অংকটা কর।

Exercise 14: Let S be a nonempty set with an associative binary operation $\star$ having identity element e. Let $a, b, c \in S$ be such that $ab = e$ and $ca = e$. Show that $b = c =$ inverse of a. ■

Associativity যে কেমন কাজের জিনিস তার একটা নমুনা রয়েছে নীচের theorem-টায়।

THEOREM

Let S be a nonempty set with a binary operation $\star$ having identity element. Let $a, b \in S$ have inverse elements a^{-1} and b^{-1}, respectively. If the binary operation is associative, then ab also has inverse and the inverse is $b^{-1}a^{-1}$.

Proof: প্রমাণটা খুবই সহজ, কিন্তু প্রথমে বলে রাখি এই theorem-টা কেন খুবই স্বাভাবিক জিনিস। বস্তুতঃ এই theorem-টা যদি না থাকত, তবে আমাদের পক্ষে প্রতিদিনের জীবনে চলাই দুষ্কর হত। জুতোমোজা পরার মত একটা সহজ জিনিসের কথাই ধরো। যদি মোজা পরাকে a, এবং জুতো পরাকে b বলি তবে a^{-1} হবে মোজা খোলা এবং b^{-1} হবে জুতো খোলা। মনে কর তুমি মোজা জুতো পরলে, মানে প্রথমে মোজা এবং তারপর জুতো পরলে। এবার যদি সেগুলো খুলতে চাও মানে $(ab)^{-1}$ করতে চাও, তবে নিশ্চয়ই প্রথমে জুতো খুলবে (b^{-1}) এবং তারপরে মোজা খুলবে (a^{-1}). সুতরাং দাঁড়ালো $(ab)^{-1} = b^{-1}a^{-1}$. এবার প্রমাণটা দেখলেই বুঝবে এর মধ্যে কোথায় associativity লাগছে--

$$\begin{aligned}(b^{-1}a^{-1})(ab) &= (b^{-1}(a^{-1}a))b \quad [\because \text{associative}] \\ &= (b^{-1}e)b \\ &= b^{-1}b = e.\end{aligned}$$

Again,

$$\begin{aligned}(ab)(b^{-1}a^{-1}) &= (a(bb^{-1}))a^{-1} \quad [\because \text{associative}] \\ &= (ae)a^{-1} \\ &= aa^{-1} = e.\end{aligned}$$

So $(ab)^{-1} = b^{-1}a^{-1}$, as required.

[Q.E.D]

DAY 12
Group

এবার কিছু abstract structure শেখা যাক। একটা abstract structure তৈরী হয় এক বা একাধিক set এবং তাদের উপর কিছু binary operation ইত্যাদি নিয়ে। গতকালই বলেছি যে, যদি binary operation-টার ধর্ম কোনো পূর্বপরিচিত binary operation-এর ধর্মের সঙ্গে খানিকটাও মিলে যায়, তবে কাজের অনেক সুবিধা হয়। গতকাল আমরা এরকম বিভিন্ন ধর্মের আলোচনা করেছি, যেগুলো সবই হল $\mathbb{Z}$-এর উপরে যোগ আর বিয়োগের ধর্ম। যদি এইসব অন্য কোনো binary operation-এও থাকে, তবে সেটা নিয়ে কাজ করা ছোটোবেলায় যোগ-বিয়োগের মতই সহজ হবে এটাই স্বাভাবিক। এই চিন্তা থেকেই আসে **group**-এর ধারণা, যেটা এবার আমরা শিখব।

Example 15: Define "group".[1] **(1997,2001)**

SOLUTION:

DEFINITION: **Group**

$(G, \star)$ is called a <u>group</u> if G is a nonempty set and $\star$ is a binary operation on G such that the following properties hold:

1. <u>Closure</u>: ie, $\forall a, b \in G a \star b \in G$,
2. <u>Associative</u>: ie, $\forall a, b, c \in G (a \star b) \star c = a \star (b \star c)$,
3. <u>Identity</u>: ie, $\exists e \in G \quad \forall a \in G a \star e = e \star a = a$,
4. <u>Inverse</u>: ie, $\forall a \in G \exists b \in G \quad a \star b = b \star a = e$.

■

যোগের যা সব ভালো ভালো গুণের কথা গতকাল শিখেছি, তারা প্রায় সবাই রয়েছে group-এর সংজ্ঞায়। খালি একটা ভালো গুণ বাদ দিয়েছি--commutative. সেটাও যদি জুড়ে দিই তবে পাব commutative group বা যার আরেক নাম **Abelian group.**

> **DEFINITION: Abelian/ commutative group**
>
> A group $(G, \star)$ is called **Abelian** or **commutative** if $\star$ is commutative, ie,
>
> $$\forall a, b \in G \quad a \star b = b \star a.$$

Group-এর উদাহরণ অনেক আছে। যেহেতু group-এর সংজ্ঞাটা integer-দের যোগের আদলেই তৈরী, তাই $(\mathbb{Z}, +)$ তো একটা group হবেই। এটা একটা Abelian group-ও বটে।
যদি কোনো $(G, \star)$-কে group দেখাতে হয়, তবে সংজ্ঞার সবগুলো শর্ত মেলাতে হয়। যদি একটাও শর্ত না মেলে তবে তৎক্ষণাৎ থেমে গিয়ে ঘোষণা করা যে এটা একটা group নয়। এই কায়দায় নীচের অংকটা করে হাত পাকিয়ে নাও।

Exercise 15: বল তো এরা কেন group নয়?
(1) $(\mathbb{N}, +)$ **(2)** $(\mathbb{N} \cup \{0\}, +)$ **(3)** $(\mathbb{Q}^c, +)$ **(4)** $(\mathbb{Z}, -)$
■

এবার আরেকটু কঠিন অংক।

Example 16: Is the set R^* of all nonzero real numbers a group with respect to the operation $\circ$ defined by

$$a \circ b = |a|b$$

for all $a, b \in \mathbb{R}^*$? Justify your answer.[3] **(1997,2001)**
SOLUTION: প্রথমে binary operation-টা বুঝে নাও। যদি $2 \circ 3$ বার করতে চাই, তবে সেটা হবে

$$2 \circ 3 = |2| \times 3 = 6.$$

একইভাবে,

$$(-2) \circ 3 = |-2| \times 3 = 6.$$

যেহেতু $|a| > 0$, তাই বুঝতেই পারছ যে, $a \circ b$-এর চিহ্ন সর্বদাই b-এর চিহ্নটাই হবে, সেখানে a-র কোনো ভূমিকা থাকবে না। অমনি সন্দেহ হওয়া উচিত যে, এখানে কোনো identity element থাকতে পারে না, কারণ b-এর জায়গায় identity element বসালে $a \circ b$ হওয়া উচিত a, সেখানে b-এর কোনো ছাপ থাকা উচিত না। কিন্তু আমাদের ক্ষেত্রে উত্তরের চিহ্নটায় সবসময়েই b-এর ছাপ থেকে যাবে।

> No, it is not a group, since there is no identity element.

এবার প্রমাণ করে দেখাই। Contradiction লাগাব--

> Let, if possible, $e \in \mathbb{R}^*$ be the identity element.
>
> Then $\forall a \in \mathbb{R}^* \quad a \circ e = a.$
>
> In particular, for $a = 1$ we should have $1 \circ e = |1|e = 1$ and so $e = 1$.

> But taking $a = -1$, we also need $|-1|e = -1$, and so $e = -1 (\Rightarrow\Leftarrow)$.

ওই "$\Rightarrow\Leftarrow$" চিহ্নটার মানে যে contradiction, অর্থাৎ অসম্ভব ঘটনা, সেটা তো জানোই। ■

এখানে notation সম্বন্ধে কয়েকটা কথা বলে নিই--

1. একটা group-কে কীভাবে লেখা হচ্ছে দ্যাখো--$(G, \star)$. ফার্স্ট ব্র্যাকেটের মধ্যে প্রথমে set-টাকে লিখেছি, তারপর কমা দিয়ে binary operation-টা। এই প্রসঙ্গে বলে রাখি যে, standard ইংরাজী বইতে কিন্তু "ফার্স্ট ব্র্যাকেট" কথাটা ব্যবহার করে না, ওর পোশাকী নাম হল parenthesis (প্যারেন্থেসিস) এবং বহুবচনে parentheses (প্যারেন্থেসেস)।
2. Binary operation-টাকে সাধারণতঃ দুই ধরণের চিহ্ন দিয়ে লেখা হয়
   - যোগ-জাতীয়, যেমন $+$ বা $\oplus$,
   - গুণ-জাতীয়, যেমন $\cdot, \bullet, \circ$ বা $\star$. কিন্তু বারবার $a \cdot b$ বা $a \star b$ ইত্যাদি লিখতে লিখতে হাত ব্যথা হয়ে যায় বলে আমরা প্রায়শঃই সংক্ষেপে খালি ab লিখি।
3. যদি binary operation-টাকে যোগের মত করে লিখি তবে inverse-কে লিখি বিয়োগের মত করে। যেমন binary operation-টা $+$ হলে a-র inverse-কে লিখি $-a$. আবার binary operation-টা $\oplus$ হলে, a-র inverse-কে লিখি $\ominus a$. আমরা $a + (-b)$-কে সংক্ষেপে $a - b$ লিখে থাকি। একইভাবে $a \ominus b$ মানে হল $a \oplus (\ominus b)$.
4. যদি binary operation-টাকে গুণের মত লিখি, তবে কোনো element a-র inverse-কে সব সময়ে লিখি a^{-1}.
5. অনেক সময়ে binary operation দিয়ে কোনো element-কে নিজের সঙ্গেই বার বার করে মেলানোর দরকার পড়ে, যেমন $a + a + \cdots + a$ বা $a \star a \star \cdots \star a$. এর জন্যও কিছু সংক্ষিপ্ত রূপ আছে। যদি binary operation-টার চিহ্ন যোগ-জাতীয় হয় তবে লিখি এইভাবে--

   $$a + a = 2a, \quad a + a + a = 3a, \text{ ইত্যাদি।}$$

   গুণ-জাতীয় চিহ্নের ক্ষেত্রে সংক্ষিপ্তরূপটা এইরকম--

   $$a \star a = a^2, \quad a \star a \star a = a^3, \text{ ইত্যাদি।}$$

Group-এর প্রচুর উদাহরণ আমাদের চারিদিকে ছড়িয়ে আছে। বোঝানোর সুবিধার জন্য তাদেরকে দু'ভাগে ভাগ করব--

1. পূর্বপরিচিত, যাদের সঙ্গে স্কুল থেকেই পরিচয়,
2. নতুন।

12.1 পূর্বপরিচিত কিছু group

পূর্বপরিচিত group-দের মধ্যে আছে $(\mathbb{Z}, +)$, $(\mathbb{R}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{C}, +)$. আরো কয়েকটা পরিচিত group তৈরী হয় গুণ করে--$(\mathbb{R} \setminus \{0\}, \times)$, $(\mathbb{Q} \setminus \{0\}, \times)$ এবং $(\mathbb{C} \setminus \{0\}, \times)$.
এদের সঙ্গে আমাদের প্রচুর পরিচয় আছে, তাই আর এদের গুণের ব্যাখ্যানা করে সময় নষ্ট করব না। খালি লক্ষ কর গুণের বেলায় inverse-টা হল ভাগ, এবং 0 দিয়ে ভাগ করা যায় না। সেই কারণে গুণ দিয়ে তৈরী group-দের বেলায় আমরা set-গুলো থেকে 0-কে সযত্নে বাদ রেখেছি।

12.2 নতুন নতুন group

এবার দেখব নতুন কিছু group. যেহেতু এরা আমাদের পূর্বপরিচিত নয়, তাই এদের ক্ষেত্রে বিস্তারিত প্রমাণের প্রয়োজন হবে। এবং এই কাজটা করতে গিয়েই বহু ছাত্রের গোল বেঁধে যায়--ঠিক কতটা বিস্তারিতভাবে লিখলে প্রমাণটাকে "যথেষ্ট বিস্তারিত" বলা

যায়? যেমন $(\mathbb{Z},+)$-কে group দেখানোর সময়ে আমরা associativity প্রসঙ্গে বলেছিলাম যে "$a+(b+c)=(a+b)+c$ হয় সে তো আমরা জানিই"। কিন্তু এইটুকু লিখলেই কি সেটাকে সম্পূর্ণ প্রমাণ বলা যায়? একদল ছাত্রকে দেখেছি কোথা থেকে শুরু করতে হবে বুঝতে না পেরে কিছুই লিখে উঠতে পারে না। আরেক দল আবার কোথায় থামতে হবে বুঝতে না পেরে প্রমাণের নামে পাতার পর পাতা আগডুম বাগডুম লিখে সময় নষ্ট করে। এই সমস্যাটা বিশেষ করে হয় associativity এবং commutativity প্রমাণ করতে গিয়ে। এই "বোঝা যাচ্ছে, কিন্তু বোঝানো যাচ্ছে না" জাতীয় সমস্যাটা গোড়াতেই নিরসন করা যাক। কাজটা তিন ধাপে করব--

1. $\mathbb{R}$-এর উপরে যোগ এবং গুণ দুজনেই associative এবং commutative. এই শর্তগুলো $\mathbb{R}$-এর সংজ্ঞার মধ্যে axiom হিসেবে বলা আছে। সুতরাং প্রমাণের কোনো দরকার নেই, খালি "standard property" বলে দিলেই চলবে।

2. যদি $\mathbb{R}$-এর সঙ্গে সম্পর্কিত কোনো set-এর উপর যোগ বা গুণ নিয়ে কাজ করি, তবে আমরা প্রমাণে $\mathbb{R}$-এর axiom-গুলো ব্যবহার করতে পারি। যেমন--

   - $(\mathbb{Z},+)$-এর বেলায় বলতে পারি যে $\mathbb{Z}\subseteq\mathbb{R}$ এবং $\mathbb{R}$-এর উপর $+$ হল associative, তাই $\mathbb{Z}$-এর উপরেও $+$ অবশ্যই associative.
   - complex addition যে associative সেটা দেখানোর জন্য শুরু করব তিনটে যে কোনো complex number নিয়ে। আমরা জানি যে একটা complex number-কে দুটো real number দিয়ে লেখা যায়--$a+\mathbf{i}b$, যেখানে $a,b\in\mathbb{R}$. সুতরাং--

     Let $z_1,z_2,z_3\in\mathbb{C}$.
     To show
     $$z_1+(z_2+z_3)=(z_1+z_2)+z_3. \qquad (*)$$
     Now,
     $$\begin{aligned} & Re(z_1+(z_2+z_3)) \\ = {} & Re(z_1)+Re(z_2+z_3) && [\text{definition of complex addition}] \\ = {} & Re(z_1)+(Re(z_2)+Re(z_3)) && [\text{definition of complex addition}] \\ = {} & (Re(z_1)+Re(z_2))+Re(z_3)) && [\text{associativity of real addition}] \\ = {} & Re(z_1+z_2)+Re(z_3)) && [\text{definition of complex addition}] \\ = {} & Re((z_1+z_2)+z_3) && [\text{definition of complex addition}] \end{aligned}$$
     Similarly,
     $$Im(z_1+(z_2+z_3))=Im((z_1+z_2)+z_3).$$
     So (*) is proved.

   একইভাবে দেখানো যায় যে, complex number-দের গুণ করাও হল associative. তবে যেহেতু আমরা হায়ার সেকণ্ডারী থেকেই complex number-দের নিয়ে কাজ করে আসছি, তাই এইসব associativity এরকম ধরে ধরে প্রমাণ না করে, কেবল "standard property of complex numbers" বলে ছেড়ে দেব।

3. অন্য সব ক্ষেত্রে associativity, commutativity ইত্যাদি সরাসরি প্রমাণ করতে হবে। সেরকম উদাহরণ আমরা শীঘ্রই দেখব।

12.2.1 Modulo group

গোড়াতেই যে তিনটে উদাহরণ করেছিলাম (থাম গোণা, সৈনিকের প্যারেড আর কাপ ওল্টানো) এদের প্রত্যেকের পিছনেই একটা করে group লুকিয়ে আছে। সেটা বলে না দিলে খুঁজে পাওয়া মুস্কিল। থাম গোণার ক্ষেত্রে group-টা হল $(G,\oplus)$,

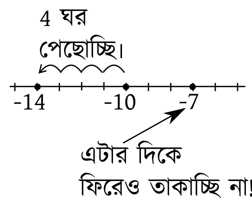


Fig 23

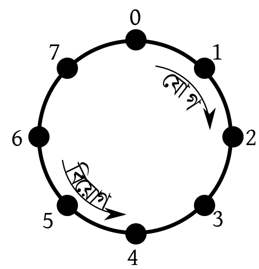


Fig 24

যেখানে $G = \{0, 1, 2, 3, 4, 5, 6\}$ এবং $a \oplus b$ মানে হল $a + b$-কে 7 দিয়ে ভাগ করে ভাগশেষ। সৈনিকের উদাহরণে $G = \{0, 1, 2, 3\}$ এবং $a \oplus b$ মানে $a + b$-কে 4 দিয়ে ভাগ করে ভাগশেষ। একইভাবে কাপ ওল্টানোর ধাঁধায় $G = \{0, 1\}$, আর ভাগশেষ নিচ্ছি 2 দিয়ে ভাগ করে। একটু চিন্তা করলেই বুঝবে এরা সবাই সত্যিই group-এর সংজ্ঞার সব কটা শর্ত পালন করে, এবং commutative-ও বটে। তিন ক্ষেত্রেই মূল যুক্তিটা একই। সেটা একবারে নীচের একটা theorem হিসেবে লিখে দিলাম। এই প্রসঙ্গে বলে রাখি যে, এই ধরণের group-দের বলে **modulo group.** যদি 4 দিয়ে ভাগ করে ভাগশেষ নাও তবে পাবে modulo-4 group, যাকে সাধারণতঃ লেখে $(\mathbb{Z}_4, \oplus)$. একইভাবে 7 দিয়ে ভাগ করে ভাগশেষ নিলে পেতাম $(\mathbb{Z}_7, \oplus)$ বা modulo-7 group.

এখানে আমরা বারবার ভাগশেষের কথা বলছি। Positive সংখ্যার ভাগশেষ বার করতে সবাই ছোটোবেলা থেকেই শেখে। কিন্তু যদি বলি -10-কে 7 দিয়ে ভাগ করলে কত ভাগশেষ থাকবে, তবে অনেকেই থতমত খেয়ে যাবে। সুতরাং এই জায়গাটা ভালো করে বুঝে নেওয়া যাক। "m-কে n দিয়ে ভাগ করলে কত ভাগশেষ থাকবে?" এই প্রশ্নটা করা হয় একমাত্র তখনই যখন n একটা positive integer, কিন্তু m যেকোনো integer, যেটা 0 বা negative হলেও আপত্তি নেই। ভাগশেষটা বার করার জন্য প্রথমে দ্যাখো m সংখ্যাটা n দিয়ে ভাগ যায় কিনা। যদি যায়, তবে ভাগশেষ 0. নইলে m থেকে শুরু করে এক এক করে পেছোতে থাকো, যতক্ষণ না প্রথম এমন একটা সংখ্যা পাও যেটা n দিয়ে ভাগ যায়। যত ঘর পিছিয়েছো সেটাই হল ভাগশেষ। এই সংখ্যাটা সব সময়েই 0 থেকে $n - 1$-এর মধ্যে থাকতে বাধ্য। সুতরাং m যদিও বা negative হয়, তার ভাগশেষ কিন্তু কখনও negative হবে না।

উদাহরণস্বরূপ -10-কে 7 দিয়ে ভাগ করে ভাগশেষ বার করা যাক। -10-থেকে এক ঘর পেছোলে -11, দুই ঘর পেছোলে -12, তিন ঘর পেছোলে -13. এখনও পর্যন্ত 7 দিয়ে ভাগ যায় না। কিন্তু যেই 4 ঘর পেছোবে অমনি পাবে $-10 - 4 = -14$, যেটা 7 দিয়ে ভাগ যায়। সুতরাং ভাগশেষ হল 4. বোঝার জন্য Fig 23 দ্যাখো।

এইবার তবে theorem-টা--

THEOREM

Let $G = \{0, 1, ..., n - 1\}$, where $n \geq 1$. For $a, b \in G$ we define $a \oplus b =$ remainder of $(a + b)$ after division by n. Then $(G, \oplus)$ is an Abelian group.

প্রমাণ করার আগে বলে নিই, এই জিনিসটাকে Fig 24-এর মত ছবি দিয়ে মনে রাখবে। এই ছবিটায় $n = 8$ দেখিয়েছি। $0, 1, ..., 7$ এই 8-টা সংখ্যাকে ঘড়ির মত করে সাজিয়েছি। এখানে যোগ (অর্থাৎ $\oplus$) মানে হল ঘড়ির কাঁটার দিকে যাওয়া। যেমন $5 \oplus 4$ করতে চাইলে 5 থেকে শুরু করে 4 ঘর ঘড়ির মত এগোও, পৌঁছবে 1-এ। সত্যিই দ্যাখো $5 \oplus 4 = 1$, কারণ $5 + 4 = 9$-কে 8 দিয়ে ভাগ করলেই ভাগশেষ হয় 1. একইভাবে বিয়োগ হল ঘড়ির কাঁটার উল্টো দিকে যাওয়া।

এবার theorem-টার প্রমাণ শেখা যাক। $a \oplus b$ হল n দিয়ে ভাগ করার পর একটা ভাগশেষ, অতএব সেটা $0, 1, ..., n - 1$-এর মধ্যে কিছু একটা হবেই। সুতরাং closure property নিয়ে কোনো সমস্যা নেই।

এখানে $a \oplus b$ হল $a + b$-এর ভাগশেষ। যেহেতু সাধারণ যোগ হল commutative, তাই $\oplus$-ও commutative হতে বাধ্য। আবার সাধারণ যোগের বেলায় identity হল 0. সুতরাং এখানেও identity হবে 0.

বাকি রইল associativity আর inverse দেখানো। এদের জন্য প্রথমে একটা জিনিস বুঝে নাও--

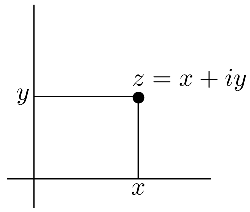


Fig 25

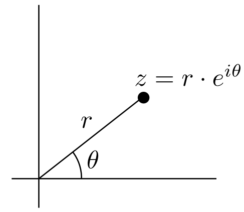


Fig 26

> যদি দুটো সংখ্যা নাও $a_1, a_2 \in \mathbb{Z}$, এবং তাদেরকে n দিয়ে ভাগ করে ভাগশেষ নিলে যথাক্রমে r_1 আর r_2 হয়, তবে $a_1 + a_2$ এবং $r_1 + r_2$ দুজনেরই সমান ভাগশেষ হবে।

কারণটা এইরকম--

> ধরো a_1, a_2-কে n দিয়ে ভাগ করলে ভাগফল হয় যথাক্রমে q_1, q_2. তাহলে $a_1 = nq_1 + r_1$ এবং $a_2 = nq_2 + r_2$. সুতরাং $a_1 + a_2 = n(q_1 + q_2) + (r_1 + r_2)$. যেহেতু $n(q_1 + q_2)$ অংশটা n দিয়ে ভাগ যায়, তাই $a_1 + a_2$ আর $r_1 + r_2$-র সমান ভাগশেষ হবে।

এইটা ব্যবহার করে associativity দেখাব এইভাবে--যা খুশি $a, b, c \in G$ নাও। তাহলে $(a \oplus b) \oplus c$ মানে $(a \oplus b) + c$-এর ভাগশেষ, আর সেটা হল $(a + b) + c$-এর ভাগশেষ। একইভাবে $a \oplus (b \oplus c)$ হল $a + (b + c)$-এর ভাগশেষ। সাধারণ যোগের associativity থেকে জানি যে, $(a + b) + c = a + (b + c)$. তাই $(a \oplus b) \oplus c$ আর $a \oplus (b \oplus c)$ দুজনেই একই জিনিসের ভাগশেষ, এবং সেই কারণে সমান।
Inverse দেখানোর জন্য যা খুশী $x \in G$ নাও। যদি $x = 0$ হয়, তবে তার inverse-ও হবে 0, কারণ $0 \oplus 0 = 0$. এটা এমনিই হল। যদি $x \neq 0$ হয়, তবে Fig 24-এর মত ছবি দিয়ে এগোব এইভাবে--0 থেকে x ঘর যাব ঘড়ির কাঁটার উল্টো দিকে। হাতেকলমে করে দেখলেই বুঝবে তুমি পৌঁছচ্ছ $n - x$-এ। সুতরাং আন্দাজ করে ফেললাম যে, x-এর inverse হবে $n - x$. প্রমাণ করার জন্য দ্যাখো $x + (n - x) = n$. আবার n দিয়ে ভাগ করলে n-র ভাগশেষ 0 হয়। তাই $x \oplus (n - x) = 0$, ঠিক যেমনটা দরকার ছিল।

12.2.2 Complex numbers: unit circle

এবার আমরা complex number দিয়ে তৈরী একটা group শিখব। এর জন্য complex number-দের ছবি দিয়ে ভাবতে পারলে সুবিধা হবে। আমরা জানি যে, $z \in \mathbb{C}$ হলে তাকে complex plane-এ একটা বিন্দু বলে কল্পনা করা যায়। যদি $z = x + \mathbf{i}y$ হয়, যেখানে $x, y \in \mathbb{R}$, তবে বিন্দুটা আঁকব (x, y)-তে। Fig 25 দ্যাখো। যদি $z \neq 0$ হয় তবে z-কে আরেকভাবেও লেখা যায়, $z = re^{\mathbf{i}\theta}$, যাকে বলে **polar form.** Fig 26 দ্যাখো। এখানে $r > 0$-কে বলে z-এর **modulus** বা $|z|$, এবং θ-কে বলে z-এর **argument**, বা $\arg(z)$. লক্ষ করো যে, $|z|$ হল origin থেকে z-এর দূরত্ব।
যদি $z_1 = r_1 e^{\mathbf{i}\theta_1}$ এবং $z_1 = r_2 e^{\mathbf{i}\theta_2}$ হয় তবে

$$z_1 z_2 = r_1 r_2 e^{i(\theta_1 + \theta_2)}.$$

অর্থাৎ modulus দুটো গুণ হয়ে গেল এবং argument দুটো যোগ হল। আমরা কাজ করব সেই সব $z \in \mathbb{C}$ নিয়ে যাদের $|z| = 1$. এরকম z-রা complex plane-এ origin-কে কেন্দ্র করে 1 radius-বিশিষ্ট circle-এর পরিধি জুড়ে থাকে (Fig 27)। একটু হাতেকলমে অংক করে গা গরম করে নিই।

Example 17: ধরো এরকম দুটো সংখ্যা নিলাম z_1, z_2, যেমন দেখিয়েছি Fig 28-তে। বলতে পারো এদের গুণফল $z_1 z_2$ কোথায় থাকবে?

SOLUTION: যেহেতু $|z_1 z_2| = |z_1| \times |z_2| = 1 \times 1 = 1$, তাই গুণফলটাও ওই circle-এর উপরেই থাকবে। এবং ওদের argument দুটো যোগ হয়ে যাবে, মানে $z_1 z_2$-এর argument হবে $30° + 60° = 90°$. সুতরাং $z_1 z_2$ হবে $\mathbf{i}$. ■

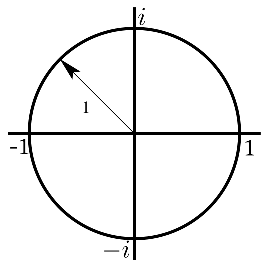


Fig 27

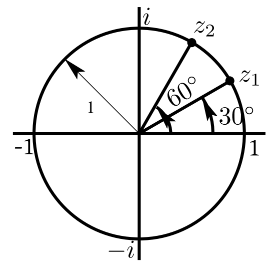


Fig 28

Example 18: Let $G = \{z : z \in \mathbb{C}, \quad |z| = 1\}$ where $\mathbb{C}$ is the set of all complex numbers. Show that G is a commutative group w.r.t. usual multiplication in $\mathbb{C}$.[5] **(2000)**

SOLUTION:

Closure: Shall show

$\forall z_1, z_2 \in G \quad z_1 z_2 \in G.$

Take any $z_1, z_2 \in G.$

Then $|z_1| = |z_2| = 1,$ and so $|z_1 z_2| = |z_1| \cdot |z_2| = 1.$

So $z_1 z_2 \in G,$ as required.

Associative:

Complex multiplication is associative (standard property).

Identity: We know that 1 is the identity element for complex multiplication.

$\because |1| = 1, \therefore 1 \in G$ is the identity here also.

Inverse: We know that for any complex $z \neq 0$ the inverse is $\frac{1}{z}$.

If $z \in G,$ then $|z| = 1,$ and so $|[|\frac{1}{z}|]| = \frac{1}{|z|} = 1.$

So $\frac{1}{z} \in G.$

Hence $\frac{1}{z}$ is the inverse of z in $G.$

Commutative:

Complex multiplication is commutative (standard property).

■

Example 19: Show that the set G of all complex numbers $a + \mathbf{i}b$ such that $a^2 + b^2 = 1$ is a group w.r.t. usual multiplication.[3] **(1997)**

SOLUTION: আগের অংকটার মতই, কারণ $z = a + \mathbf{i}b$ হলে $a^2 + b^2 = 1$ মানে $|z| = 1.$ ■

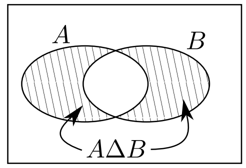


Fig 29

12.2.3 Power set

এবার আমরা একটা সম্পূর্ণ নতুন ধরণের group-এর কথা শিখব। ধরো একটা set নিলাম--S. এর যতগুলো subset আছে তাদের set-টাকে বলে **power set** of A. যেমন $S = \{1, 2\}$ নিলে power set-টা হবে

$$\mathscr{P}(S) = \big\{\phi, \quad \{1\}, \quad \{2\}, \quad \{1,2\}\big\}.$$

এই power set-এর উপর একটা binary operation শিখেছিলাম, যার নাম symmetric difference. যদি $A, B \in \mathscr{P}(S)$ নিই তবে ওদের symmetric difference-কে লেখে $A\Delta B$ যার সংজ্ঞা ছিল

$$A\Delta B = (A \cap B^c) \cup (A^c \cap B).$$

Fig 29 দ্যাখো। $A\Delta B$ হল S-এর সেইসব element দিয়ে তৈরী যারা A, B-র মধ্যে ঠিক একজনের ভিতরে আছে। মজার কথা হচ্ছে $(\mathscr{P}(S), \Delta)$ একটা Abelian group হয়! সেটাই নীচের theorem-টার বক্তব্য।

> THEOREM
>
> Let S be any set. Let $\mathscr{P}(S)$ be its power set, and let Δ denote the symmetric difference operation. Then $(\mathscr{P}(S), \Delta)$ is an Abelian group.

ধরে ধরে কষে গেলেই এটাকে প্রমাণ করে দেওয়া যায়। যুক্তির দিক দিয়ে জটিল কিছুই নয়, খালি লম্বা হবে। তাই আর প্রমাণটা দিলাম না।

এই group-টা আমাদের বিভিন্ন কাজে লাগবে। এর একটা বৈশিষ্ট্য আছে--যদি $A \in \mathscr{P}(S)$ হয় তবে $A\Delta A = \phi$, বা group-এর ভাষায় $A^2 = e$. লক্ষ কর যে, S-এর সাইজ যদি n হয়, তবে $\mathscr{P}(S)$-এর সাইজ হবে 2^n. এর মধ্যে $n = 2$ হলে এই group-টার একটা বিশেষ নাম আছে--একে বলে **Klein's 4-group.** নামটা দেওয়া হয়েছে Felix Klein (ফেলিক্স ক্লাইন) বলে একজন গণিতজ্ঞের নামে। Klein's 4-group-কে সংক্ষেপে লেখে K_4. এর সাইজ হল $2^2 = 4$. নীচের অংকটা এই K_4-এর সঙ্গে একটু পরিচিত হবার জন্যে দিলাম।

Exercise 16: ধরো $S = \{1, 2\}$. তাহলে আমরা জানি যে

$$\mathscr{P}(S) = \big\{\phi, \quad \{1\}, \quad \{2\}, \quad \{1,2\}\big\}.$$

এখানে binary operation-এর (মানে symmetric difference-এর) নামতাটা লিখে ফেলতে পারো?

HINT:

খানিকটা লিখে দিলাম। বাকিটা তুমি পূর্ণ কর।

	ϕ	$\{1\}$	$\{2\}$	$\{1,2\}$
ϕ	ϕ	$\{1\}$	$\{2\}$	$\{1,2\}$
$\{1\}$	$\{1\}$	ϕ	?	$\{2\}$
$\{2\}$	?	?	?	?
$\{1,2\}$	?	?	?	?

■

12.3 কিছু সহজ অংক

আমরা বারবারই বলেছি যে, group ব্যাপারটা তৈরী হয়েছে ছোটোবেলার স্কুলে শেখা যোগ-বিয়োগের আদলে। উদ্দেশ্য হল, যোগ-বিয়োগের যেসব ধর্ম আমাদের মজ্জাগত হয়ে গেছে, সেগুলো যে কোনো group-এর ক্ষেত্রেই লাগানো যাবে। এবার তার কিছু উদাহরণ দেখব।
ধরো ছোটোবেলার এই অংকটা--

রামের চেয়ে রহিম 5 বছরের বড়। রহিমের বয়স যদি 15 বছর হয়, তবে রামের বয়স কত হবে?

স্কুলে অংকটা আমাদের এইভাবে করতে শেখানো হয়--ধরি রামের বয়স x বছর। তাহলে রহিমের বয়স $x+5$ বছর। সুতরাং $x+5=15$. এইবার আমাদের একটা "ম্যাজিক" শেখানো হয়--বাঁদিকের ওই $+5$-টাকে ডানদিকে নিয়ে আসতে হয়, এবং তখন আবার প্লাসটা কেন যেন মাইনাস হয়ে যায়--$x=15-5=10$. এই "ম্যাজিক"-টা কেন কাজ করে, সেটা স্কুলে পড়ার সময়ে অনেকের কাছেই স্পষ্ট হয় না। কিন্তু অন্ধের মত করে গেলে অংকগুলো দিব্যি মিলে যায়। Group-এর বেলাতেও একই রকম ম্যাজিক খাটে। সেটাই নীচের অংকটাতে আমরা দেখব।

Example 20: True or false: In a group $(G,\bullet)$ if $a\bullet b=a\bullet c$, then $b=c$.[2] **(2000)**

SOLUTION: এই অংকটা যে ছোটোবেলার স্কুলের অংকেরই রকমফের সেটা কি দেখতে পাচ্ছ? খালি $\bullet$-র জায়গায় $+$ কল্পনা কর। এবার যদি b,c-কে বলি যথাক্রমে রাম এবং রহিমের বয়স, আর a-কে নিই যা খুশী কোনো সংখ্যা (ধরো 5) তবে আমাদের অংকটা স্কুলের ভাষায় দাঁড়ায় এরকম--5 বছর পরে যদি রাম আর রহিমের বয়স সমান হয়, তবে বল তো এখনও ওদের বয়স সমান কিনা। মানে $a+b=a+c$ থেকে দেখাতে হবে $b=c$. "ম্যাজিক" কায়দাটা হল সমীকরণটার দু দিক থেকেই a "কেটে দেওয়া"। মুস্কিল হল "কেটে দেওয়া" বলে কোনো ব্যাপার তো group-এর সংজ্ঞার মধ্যে নেই। সুতরাং আমাদের প্রথম কাজ হবে group-এর সংজ্ঞা থেকে "কেটে দেওয়া" (যাকে ইংরাজীতে বলে **cancellation law**) সেইটা অবধি পৌঁছনো। প্রশ্নে যে সমীকরণটা দিয়েছে সেটা হল

$$a\bullet b=a\bullet c.$$

লক্ষ কর যে, এর দুই দিকেই a রয়েছে একেবারে বাঁপাশে। এবার বাঁদিক থেকে a-কে "কেটে দেওয়া" মানে হল সমীকরণটার দুই দিককে a^{-1} দিয়ে গুণ করা (এখানে গুণ বলতে অবশ্যই আমরা $\bullet$ operation-টা বোঝাচ্ছি)। এই ব্যাপারটাকেই ব্যাখ্যানা করে লিখব--

> The statement is true.
> Let e be the identity of G.
> We are given
> $$a\bullet b=a\bullet c.$$
> Multiplying both sides from the left by a^{-1},
> $$a^{-1}\bullet(a\bullet b)=a^{-1}\bullet(a\bullet c),$$

> or, by associativity,
> $$(a^{-1} \bullet a) \bullet b = (a^{-1} \bullet a) \bullet c,$$
> and so, by definition of a^{-1},
> $$e \bullet b = e \bullet c,$$
> or since e is the identity,
> $$b = c,$$
> as required.

অংকটাকে ঠিক কঠিন বলা যায় না, কিন্তু নয় নয় করেও বেশ কয়েক লাইন হল, কারণ আমরা প্রতিটা ধাপ group-এর সংজ্ঞা থেকে সরাসরি দেখিয়েছি। মূল যুক্তিটা ছোটোবেলার স্কুলের অংকের মত হলেও একটা গুরুত্বপূর্ণ পার্থক্য আছে--এখানে $\bullet$-টা commutative নাও হতে পারে। তাই $a \bullet b = a \bullet c$-তে দুই দিকেই যে a-টা একইপাশে আছে, সেটা খুব গুরুত্বপূর্ণ। কিন্তু যদি $b \bullet a = a \bullet c$ দেওয়া থাকত, তবে মোটেই দুদিক থেকে a-কে "কেটে দেওয়া" চলত না। ■

বাঁদিক থেকে এই যে "কেটে দেওয়া" গেল, একে বলে left cancellation law. একইভাবে একটা right cancellation law-ও আছে, যেটা নিয়ে নীচের অংকটা।

Exercise 17: Prove the right cancellation law in a group: If G is a group and $a, b, c \in G$ then

$$ab = cb \implies a = c.$$

■

ছোটোবেলা থেকেই শুনে আসছি যে, "মাইনাসে মাইনাসে প্লাস" হয়। সে ব্যাপারটা যে কোনো group-এর ক্ষেত্রেও হয়। অবশ্য group-এর বেলায় "মাইনাস" না বলে আমরা বলি inverse. তাই এখানে যেটা হয় সেটা হল--কোনো element-এর inverse-এর inverse আবার সেই গোড়ার element-টাই হয়। কেন হয়, সেটাই দেখাতে বলেছে নীচের অংকটায়।

Example 21: In a group G prove that $\left(a^{-1}\right)^{-1} = a$ where $a \in G$.[2] **(1999)**

SOLUTION:

> Let $a \in G$ and $b = a^{-1}$.
> To show that $b^{-1} = a$, ie, $ab = ba = e$.
> Now $ab = aa^{-1} = e$, and $ba = a^{-1}a = e$, as required.

■

এর পরের অংকটায় একটা নতুন কথা আছে--**idempotent.** যদি S যেকোনো একটা set এবং $\star$ তার উপরে যে কোনো একটা binary operation হয়, তবে কোনো $a \in S$-কে idempotent বলব যদি $a \star a = a$ হয়। যেমন $\mathbb{Z}$-এর মধ্যে $+$-এর জন্য idempotent খালি একজনই--$0 + 0 = 0$. কিন্তু গুণের বেলায় দুজন আছে idempotent– $0 \times 0 = 0$ এবং $1 \times 1 = 1$.

Example 22: True or false: The identity element is the only idempotent element in a group.[2]

(2002,2008)

SOLUTION:

> The statement is true,

মনে রেখো যে, এখানে আমাদের দুটো জিনিস দেখাতে হবে। এক, identity একটা idempotent element, এবং দুই, idempotent element মাত্রেই identity হতে বাধ্য।

> because $e^2 = e$,
> and if $a^2 = a$ then left multiplying both sides by a^{-1} we have $a^{-1}a^2 = a^{-1}a$, or $a^{-1}(aa) = e$, or, by associativity, $(a^{-1}a)a = e$, or $ea = e$, or $a = e$, as required.

■

DAY 13
Matrix groups

গতকালই আমরা বেশ কিছু নতুন নতুন group-এর কথা শিখেছি। আজকে এবং পরশু সেই তালিকাকে আরো দীর্ঘ করব। এত এত group দেখে একসময়ে মাথা ধরে যাবার উপক্রম হতে পারে। তাই গোড়াতেই অভয় দিয়ে রাখি যে, এ অংকগুলো নিতান্তই কিছু পরীক্ষা-মার্কা কসরৎ, group theory শেখার পথে সহায়ক তো নয়ই, বরং বিরক্তি উৎপাদন করে উৎসাহ কমিয়ে দেয়। যাদের পরীক্ষাপাশের তাড়া নেই, তারা এগুলো খুব হাল্কা করে দেখে ছেড়ে দিতে পারো।
আজকের উদাহরণগুলোতে আমরা কাজ করব square matrix-দের নিয়ে, এবং binary operation-টা হবে matrix multiplication. সুতরাং matrix multiplication যে associative, সেই কথাটা বার বার কাজে লাগবে। এটা একটা standard জিনিস, তাই এখানে প্রমাণ করছি না।

Example 23: Show that the set of 2×2 real orthogonal matrices forms a group w.r.t. matrix multiplication. Show that this group is not commutative.[4+1] **(2004)**
SOLUTION: প্রথমে মনে করে নিই orthogonal matrix-এর সংজ্ঞাটা কী ছিল। একটা matrix আছে ধরো A. একে আমরা orthogonal বলব যদি $A'A = A'A = I$ হয়, মানে A'-ই A^{-1}-ও হয়। তার মানে এই অংকে আমাদের set-টা এইরকম--

> The set of all 2×2 real orthogonal matrices is
> $$G = \{A_{2\times 2} : A'A = I\},$$
> where A' denotes the transpose of A.

এবার দেখা যাক G-কে group প্রমাণ করতে কী কী দেখাতে হবে। প্রথমে দেখাতে হবে closure property, অর্থাৎ G-এর দুটো element-কে গুণ করলে সত্যিই গুণফলটা G-এর ভিতরেই থাকে। তারপর দেখাতে হবে operation-টা associative এবং এর একটা identity element আছে, এবং প্রতিটি element-এর একটা inverse আছে। এখানে আমরা একটা জিনিস ব্যবহার করব--যদি A, B দুটো matrix হয়, তবে

$$(AB)' = B'A'.$$

আমরা সাধারণতঃ আগে closure এবং তারপরে associativity দেখাই। কিন্তু এখানে closure প্রমাণ করতে associativity লাগবে। তাই associativity দিয়ে শুরু করি--

Associative: Matrix multiplication is associative, by standard result.

এইবার closure. এখানে দেখাতে হবে--যদি A আর B দুজনেই orthogonal হয়, তবে AB-ও orthogonal হবে, মানে $(AB)'(AB) = (AB)'(AB) = I$ হবে।

Closure:

If $A, B \in G$, then AB is a 2×2 matrix such that, by associativity,

$$\begin{aligned} (AB)'(AB) &= (B'A')(AB) \quad [\because (AB)' = B'A'] \\ &= B'(A'A)B \quad [\text{by associativity}] \\ &= B'IB \quad [\because A'A' = I] \\ &= B'B \\ &= I \quad [\because B'B = I]. \end{aligned}$$

Similarly,

$$(AB)(AB)' = (AB)(B'A') = A(BB')A' = AA' = I.$$

So $AB \in G$.

সুতরাং গুণফলটা G-এর মধ্যেই রইল।
এবার identity দেখানোর পালা। Matrix multiplication-এর ক্ষেত্রে identity হল identity matrix-টা। খালি দেখিয়ে দেব যে, সেটা G-এর মধ্যে আছে।

Identity:

The identity matrix

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in G,$$

because $I'I = II = I$.

এবার inverse দেখাতে হবে। মনে রেখো যে, orthogonal matrix-দের ক্ষেত্রে transpose-টাই হল inverse.

Inverse:

For $A \in G$ we have $A'A = AA' = I$. So $A^{-1} = A'$.

Now $A' \in G$ because

$$(A')'A' = AA' = I.$$

এবার অংকের দ্বিতীয় অংশ। Non-commutative দেখাতে হবে, মানে এমন দুটো $A, B \in G$ বার করতে হবে যাতে $AB \neq BA$ হয়। Matrix multiplication যে commutative নয়, সে তো আমরা জানিই, খালি সমস্যা হল $A, B \in G$ বার করা। চট্ করে ইচ্ছে মত 2×2 সাইজের orthogonal matrix বানানোর একটা সহজ কায়দা আছে। প্রথমে যে কোনো দুটো সংখ্যা নাও $a, b \in \mathbb{R}$. সমান হলেও আপত্তি নেই, খালি দুজনেই যেন শূন্য না হয়ে যায়। এদের দিয়ে একটা matrix বানাও--

$$\begin{bmatrix} a & b \\ b & -a \end{bmatrix}.$$

যদি একে $\sqrt{a^2+b^2}$ দিয়ে ভাগ করে দাও তবেই একটা orthogonal matrix পাবে--

$$\frac{1}{\sqrt{a^2+b^2}}\begin{bmatrix} a & b \\ b & -a \end{bmatrix}.$$

একটু চিন্তা করলেই দেখবে যে, যাই a, b নাও না কেন, এটা একটা orthogonal matrix. [1]

<u>Not commutative:</u> Take

$$A = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \text{ and } B = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}.$$

কী করে এদের পেলাম বুঝতেই পারছ। A-র বেলায় $a = b = 1$ নিয়েছিলাম, আর B-র বেলায় $a = -1, b = 0$.

Then $A, B \in G$ and

$$AB = \frac{1}{\sqrt{2}}\begin{bmatrix} -1 & 1 \\ -1 & -1 \end{bmatrix},$$

but

$$BA = \frac{1}{\sqrt{2}}\begin{bmatrix} -1 & -1 \\ 1 & -1 \end{bmatrix}.$$

Thus, $AB \neq BA$.

আচ্ছা, কী করে বুঝলাম যে, ঠিক এই দুটো A, B-তেই কাজ হবে, মানে $AB \neq BA$ হবে? উত্তর হল--স্রেফ আন্দাজে! খুব সহজ কোনো a, b না নিলে অধিকাংশ ক্ষেত্রেই $AB \neq BA$ হয়। চাইলে তুমি A-এর জন্য $a = 23, b = -45$ আর B-র জন্য $a = 4, b = -99$ নিয়ে দেখতে পারো। বা অন্য যা খুশী বিদঘুটে a, b. ■

Example 24: Prove that the set S is a group under matrix multiplication, where S is the set of all 2×2 real matrices $\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}$ with $ac \neq 0$. Is it commutative?[4+1] **(2005)**

SOLUTION:

Here

$$M = \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \ : \ a, b, c \in \mathbb{R}, \quad ac \neq 0 \right\}.$$

<u>Closure:</u>

If

$$A = \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \text{ and } B = \begin{bmatrix} p & q \\ 0 & r \end{bmatrix} \in M$$

then $ac \neq 0$ and $pr \neq 0$.

So

$$AB = \begin{bmatrix} a & b \\ 0 & c \end{bmatrix}\begin{bmatrix} p & q \\ 0 & r \end{bmatrix} = \begin{bmatrix} ap & aq + br \\ 0 & cr \end{bmatrix},$$

[1] আরও অনেকখানি চিন্তা করলে এও দেখবে যে, যে কোনো 2×2 orthogonal matrix-কেই এইভাবে পাওয়া যায়। এই তথ্যটা এখানে অবশ্য দরকার হবে না।

where $(ap)(cr) = (ac)(pr) \neq 0$.
Hence $AB \in M$.

Associativity:

Matrix multiplication is associative, by standard property.

এবার identity দেখাবো। তার জন্য এটা দেখানোই যথেষ্ট যে $identitymatrix$-টা আমাদের set-এর মধ্যে আছে--

Identity:

Identity matrix $I \in M$, taking $a = c = 1$ and $b = 0$.

Inverse-এর ক্ষেত্রে মনে রেখো যে

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \frac{1}{ad - bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

Inverse:

If $A = \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \in M$ then $det(A) = ac \neq 0$.
So A^{-1} exists,

$$A^{-1} = \frac{1}{ac} \begin{bmatrix} c & -b \\ 0 & a \end{bmatrix} = \begin{bmatrix} \frac{1}{a} & -b \\ 0 & \frac{1}{c} \end{bmatrix} \in M,$$

Since

$$\frac{1}{a} \times \frac{1}{c} = \frac{1}{ac} \neq 0.$$

Hence M is indeed a group w.r.t. matrix multiplication, as required.

এবার দ্বিতীয় অংশ--

No, this group is not commutative, because if

$$A = \begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} \text{ and } B = \begin{bmatrix} 2 & 3 \\ 0 & 4 \end{bmatrix}$$

then $A, B \in M$ and

$$AB = \begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} \begin{bmatrix} 2 & 3 \\ 0 & 4 \end{bmatrix} = \begin{bmatrix} 2 & 11 \\ 0 & 12 \end{bmatrix}.$$

But

$$BA = \begin{bmatrix} 2 & 3 \\ 0 & 4 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} = \begin{bmatrix} 2 & 13 \\ 0 & 12 \end{bmatrix} \neq AB.$$

■

নীচের অংকটা একইরকম। হাত পাকানোর জন্য দিলাম।

Exercise 18: Let G be the set of all 2×2 invertible matrices with $(1,2)$-th entry equal to 0. Show that G is a group under matrix multiplication. ■

Example 25: Let

$$G=\left\{\begin{bmatrix}1 & n\\ 0 & 1\end{bmatrix} : n \text{ is an integer}\right\}.$$

Show that G is a group w.r.t. the usual matrix multiplication. Is this group commutative? Justify your answer.[5] **(1998)**

SOLUTION:

> <u>Closure:</u>
>
> Take any
>
> $$\begin{bmatrix}1 & m\\ 0 & 1\end{bmatrix}, \begin{bmatrix}1 & n\\ 0 & 1\end{bmatrix}\in G.$$
>
> Then $m, n\in\mathbb{Z}$. So
>
> $$\begin{bmatrix}1 & m\\ 0 & 1\end{bmatrix}\begin{bmatrix}1 & n\\ 0 & 1\end{bmatrix}=\begin{bmatrix}1 & m+n\\ 0 & 1\end{bmatrix}\in G,$$
>
> since $m+n\in\mathbb{Z}$.

Associativity তো standard property আছেই--

> <u>Associative:</u> Standard property of matrix multiplication.

এবার identity দেখানোর পালা--

> <u>Identity:</u>
>
> Taking $n=0$
>
> $$I=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}=\begin{bmatrix}1 & n\\ 0 & 1\end{bmatrix}\in G.$$

অবশেষে inverse--

> <u>Inverse:</u>
>
> If
>
> $$\begin{bmatrix}1 & n\\ 0 & 1\end{bmatrix}\in G$$
>
> then
>
> $$\begin{bmatrix}1 & n\\ 0 & 1\end{bmatrix}^{-1}=\frac{1}{1\times 1-0\times n}\begin{bmatrix}1 & -n\\ 0 & 1\end{bmatrix}=\begin{bmatrix}1 & -n\\ 0 & 1\end{bmatrix}\in G,$$

> Since $-n \in \mathbb{Z}$.

এবার দ্বিতীয় অংশ--

> Yes, this group is commutative, because for any
>
> $$\begin{bmatrix} 1 & m \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \in G,$$
>
> we have
>
> $$\begin{bmatrix} 1 & m \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & m+n \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & m \\ 0 & 1 \end{bmatrix}.$$

একটা জিনিস লক্ষ কর--যদিও matrix multiplication মোটেই commutative নয়, কিন্তু তাও এই group-টা commutative হল। কারণ যখন বলছি যে, matrix multiplication ব্যাপারটা commutative নয়, তার মানে এই নয় যে, সব A, B-র জন্যই $AB \neq BA$ হয়। এর মানে শুধু এই যে, এমন বিট্‌কেল A, B পাওয়া সম্ভব, যাতে $AB \neq BA$ হয়। কিন্তু এই অংকে আমরা তো আর যাবতীয় matrix নিয়ে কাজ করছি না। আমরা কাজ করছি খালি $\begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}$ চেহারার matrix-দের নিয়ে। দেখা যাচ্ছে যে, সৌভাগ্যক্রমে এই চেহারার matrix-রা কেউ বিট্‌কেল হতে পারে না। সেই কারণে G দিব্যি একটা commutative group হতে পারছে। ■

এইরকম আরেকটা অংক কর।

Exercise 19: Show that the set of all diagonal invertible $n \times n$ matrices forms an Abelian group under matrix multiplication.
HINT: Abelian মানে যে commutative সেটা নিশ্চয়ই মনে আছে? ■

Example 26:

$$M = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \;:\; ad - bc = 2^n, \quad n \in \mathbb{Z} \right\}.$$

Verify whether M is a group with respect to matrix multiplication. Cite an example to show that it is non-Abelian.[5] **(2007)**
SOLUTION: সমাধানটা সহজে লেখার জন্য আমরা দুটো তথ্য ব্যবহার করব--

- এক, $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ হলে $det(A) = ad - bc$ হয়।
- দুই, $det(AB) = det(A)det(B)$ হয়।

> Here
>
> $$M = \{A_{2\times 2} \;:\; det(A) = 2^n, \quad n \in \mathbb{Z}\}.$$
>
> Closure property:
>
> If $A, B \in M$ then $det(A) = 2^m$ and $det(B) = 2^n$ for some $m, n \in \mathbb{Z}$.
> So $det(AB) = det(A)det(B) = 2^{m+n}$.

> Hence $AB \in M$, because $m+n \in \mathbb{Z}$.
> Associativity:
> Matrix multiplication is associative (standard property).

এবার identity-র পালা--

> Identity:
> Identity matrix $I \in M$, since $det(I) = 1 = 2^0$.

খালি inverse দেখানো বাকি--

> Inverse:
> If $A \in M$ then $det(A) = 2^n (\neq 0)$ for some $n \in \mathbb{Z}$.
> So A^{-1} exists, and $det(A^{-1}) = 1/det(A) = 2^{-n}$.
> Thus, $A^{-1} \in M$, since $-n \in \mathbb{Z}$.

এবার দ্বিতীয় অংশ।

> This group is not commutative, because if
>
> $$A = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} \text{ and } B = \begin{bmatrix} 4 & 9 \\ 0 & 16 \end{bmatrix}$$
>
> then $A, B \in M$ and
>
> $$AB = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} \begin{bmatrix} 4 & 9 \\ 0 & 16 \end{bmatrix} = \begin{bmatrix} 4 & 9 \\ 0 & 32 \end{bmatrix}.$$
>
> But
>
> $$BA = \begin{bmatrix} 4 & 9 \\ 0 & 16 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} = \begin{bmatrix} 4 & 18 \\ 0 & 32 \end{bmatrix} \neq AB.$$

■

Example 27: True or false? Justify.

$$M_2 = \left\{ \begin{bmatrix} 2^m & 0 \\ 0 & 3^n \end{bmatrix} : m, n \text{ nonzero integers} \right\}.$$

M_2 forms a group w.r.t. matrix multiplication.[2] **(2003)**
SOLUTION: আগে চট্ করে বুঝে নিই group হবে কি হবে না। তার জন্য মনে মনে চারটে শর্তকে পরীক্ষা করে দেখতে হবে। যদি অন্ততঃ একটাও পালিত না হয়, তবে সেটা লিখে দিলেই প্রমাণ হয়ে যাবে যে group নয়। যদি সবগুলো শর্তই

পালিত হয়, তবে সবাইকে আলাদা করে প্রমাণ করতে হবে। সুতরাং বুদ্ধিমানের কাজ হল যে শর্তগুলো মনে মনে পরীক্ষা করে দেখা সবচেয়ে সহজ তাদের নিয়ে শুরু করা। প্রথমেই দেখি closure আছে কিনা। যদি দুটো matrix নিই এইরকম--

$$A = \begin{bmatrix} 2^{m_1} & 0 \\ 0 & 3^{n_1} \end{bmatrix} \text{ আর } B = \begin{bmatrix} 2^{m_2} & 0 \\ 0 & 3^{n_2} \end{bmatrix},$$

তবে পাব

$$AB = \begin{bmatrix} 2^{m_1+m_2} & 0 \\ 0 & 3^{n_1+n_2} \end{bmatrix}.$$

এখানে প্রশ্নের শর্ত অনুযায়ী $m_1, m_2, n_1, n_2 \neq 0$ নিয়ে শুরু করলেও $m_1 + m_2 \neq 0$ আর $n_1 + n_2 \neq 0$ হবার কোনো গ্যারান্টি নেই। সুতরাং closure থাকছে না। সেটাই এবার গুছিয়ে একটা counterexample হিসেবে লিখব।

> The statement is false.
> Let
> $$A = \begin{bmatrix} 2 & 0 \\ 0 & 3 \end{bmatrix} \text{ and } A = \begin{bmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{3} \end{bmatrix}.$$
> Then $A, B \in M_2$, but
> $$AB = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 2^0 & 0 \\ 0 & 2^0 \end{bmatrix} \notin M_2.$$
> Hence M_2 is not closed under matrix multiplication.

■

একইরকম দেখতে আরেকটা অংক দিচ্ছি এবার, এখানে কিন্তু একটু প্যাঁচ আছে।

Example 28:

$$M_2 = \left\{ \begin{bmatrix} x & y \\ x & y \end{bmatrix} : x, y \in \mathbb{R} \text{ and } x + y \neq 0 \right\}.$$

Does M_2 form a group with respect to matrix multiplication? Justify. ($\mathbb{R}$ denotes the set of real numbers.)[3] **(2008)**

SOLUTION: এখানে closure পরীক্ষা করে দেখতে পারো, কোনো সমস্যা পাবে না। সমস্যা বাঁধবে identity নিয়ে। এবং প্যাঁচটা সেখানেই। যদি তুমি ফস্ করে লিখে দাও--

> "Identity matrix আমরা জানি $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, যেটা মোটেই $\begin{bmatrix} x & y \\ x & y \end{bmatrix}$ আকারের নয়, তাই M_2-র কোনো identity নেই।"

তবে কিন্তু সেটা সঠিক যুক্তি হবে না। কারণ যদি $I \in M_2$ হত তবে সেটাই M-এর identity হতে বটে, কিন্তু $I \notin M_2$ হলেও M_2-এর মধ্যে M_2-র নিজস্ব কোনো identity element থাকতে পারে। কথাটা স্পষ্ট না হলে এই উদাহরণটা ভাবো--ধরো $M = \left\{ \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \right\}$, অর্থাৎ M একটা singleton set, যার মধ্যে স্রেফ zero matrix-টা আছে, আর কিচ্ছু নেই। এই M-টা কিন্তু দিব্যি একটা group হবে, যেখানে operation-টা হল matrix multipication. এখানে ওই zero matrix-টাই M-এর নিজস্ব identity element. এখানে তুমি যদি বলে বসো--"$I \notin M$ তাই M একটা group হতে পারে না", তবে সেটা ভুল হবে।

এখানেও তেমনি আমাদের সাবধানে দেখতে হবে M_2-র নিজস্ব কোনো identity element আছে কিনা।

No M_2 is not a group with respect to matrix multiplication.

Let, if possible M be a group. Then it must have an identity element

$$E = \begin{bmatrix} a & b \\ a & b \end{bmatrix}, \text{ say,}$$

with $a+b \neq 0$.

So $\forall A \in M_2$ we should have $AE = A$.

Let $A = \begin{bmatrix} x & y \\ x & y \end{bmatrix}$ with $x+y \neq 0$.

Then $AE = A$ means

$$AE = \begin{bmatrix} x & y \\ x & y \end{bmatrix} \begin{bmatrix} a & b \\ a & b \end{bmatrix} = \begin{bmatrix} ax+ay & ax+ay \\ bx+by & bx+by \end{bmatrix} = \begin{bmatrix} x & y \\ x & y \end{bmatrix},$$

In particular $ax+ay = x$.

Since this must hold for all x, y with $x+y \neq 0$,

we can put $x=1, y=0$ to get $a=1$. But, putting $x=0, y=1$ we have $a = 0 (\Rightarrow\Leftarrow)$.

Thus, M_2 has no identity element.

Hence M_2 cannot be a group under matrix multiplication.

■

DAY 14
আরও নানা রকম group

আজকে আরো কিছু পরীক্ষা-মার্কা অংক। পরীক্ষার চিন্তা না থাকলে হাল্কা করে চোখ বুলিয়ে যাও।
আজকের অংকগুলোতে binary operation-গুলো কোনো পরিচিত কিছু নয়। অংকগুলো মোটামুটি সহজই, কোথাও কোনো প্যাঁচ নেই। যারা খুঁটিয়ে পড়ছ, তারা প্রত্যেকটা অংক প্রথমে নিজে কষার চেষ্টা কর, তারপর সমাধানটা দেখো।

Example 29: Show that $G = (-1, 1)$ is a group under the operation $\bullet$ defined by

$$a \bullet b = \frac{a+b}{1+ab}.$$

SOLUTION:

<u>Closure:</u> To show

$$\forall a, b \in G \quad a \bullet b \in G.$$

$\forall a, b$

Take any $a, b \in G$.

Then $a, b \in (-1, 1)$.
To show $a \bullet b \in (-1, 1)$, ie,

$$-1 < \frac{a+b}{1+ab} < 1,$$

ie,

$$-1 - ab < a + b < 1 + ab,$$

since $1 + ab > 0$.
The first inequality is

$$-1 - a < b + ab,$$

or

$$-(1+a) < b(1+a),$$

or, since $1 + a > 0$,

$$-1 < b,$$

which is true.
Similarly, the second inequality is

$$b - ab < 1 - a,$$

or, since $1 - a > 0$,

$$b < 1,$$

which is true.
Associativity : To show

$\forall a, b, c \in G \quad (a \bullet b) \bullet c = a \bullet (a \bullet c)$.

$\forall a, b, c$ Take any $a, b, c \in (-1, 1)$.

Then

$$\begin{aligned} a \bullet (b \bullet c) &= a \bullet \left[\frac{b+c}{1+bc}\right] \\ &= \cdots \\ &= \frac{a+b+c+abc}{1+ab+bc+ca}. \end{aligned}$$

এখানে মাঝের সোজা কয়েকটা ধাপ ডট্ ডট্ দিয়ে বাদ দিয়েছি।

Also,

$$(a \bullet b) \bullet c = \cdots = \frac{a+b+c+abc}{1+ab+bc+ca},$$

as before.

এবার identity দেখাতে হবে।

Identity: Shall show

$\exists e \in G \quad \forall a \in G \quad e \bullet a = a \bullet e = a.$

Identity যদি e হয় তবে আমাদের দরকার যাতে যেকোনো a-র জন্যই $\frac{a+e}{1+ae} = a$ হয়। এই equation-টা solve করলেই দেখবে যে $e = 0$ হতে হবে।

$\exists e$ Choose $e = 0$.

$\forall a$ Take any $a \in G$.

Then

$$e \bullet a = a \bullet e = \frac{a+0}{1+a \times 0} = a,$$

as required.

এবার inverse-এর পালা।

Inverse: Shall show

$\forall a \in G \quad \exists b \in G \quad a \bullet b = b \bullet a = e.$

$\forall a$ Take any $a \in G$.

যদি a-র inverse b হয় তবে $\frac{a+b}{1+ab} = 0$ হতে হবে। Solve করলেই দেখবে যে $b = -a$ না নিয়ে পথ নেই।

$\exists b$ Choose $b = -a \in G$.

Then

$$b \bullet a = a \bullet b = \frac{a-a}{1-a^2} = 0 = e,$$

as required.

■

Example 30: Let $S = \{(a, b) : a \neq 0, a, b \in \mathbb{R}\}$ and the operation $\circ$ be defined on S as

$$(a, b) \circ (c, d) = (ac, bc + d).$$

Show that $(S, \circ)$ forms a group. Is it commutative?[4+1] **(2003)**

SOLUTION:

Closure: For any $(a, b), (c, d) \in S$,

$$(a, b) \circ (c, d) = (ac, bc + d) \in S,$$

because $ac, bc + d \in \mathbb{R}$ and $ac \neq 0$ (since $a, c \neq 0$).

Associative:

> For any $(a,b),(c,d),(e,f) \in S$,
> $$((a,b)\circ(c,d))\circ(e,f) = (ac, bc+d)\circ(e,f) = (ace, bce+de+f),$$
> and
> $$(a,b)\circ((c,d)\circ(e,f)) = (a,b)\circ(ce, de+f) = (ace, bce+de+f),$$
> as above.

(e_1, e_2) যদি identity হয়, তবে যে কোনো $(a,b) \in S$-এর জন্যই $(e_1 a, e_2 a + b) = (a,b)$ হতে হবে। তার মানে $e_1 = 1$ আর $e_2 = 0$ হতেই হবে।

> Identity: $(1,0) \in S$ is the identity because for any $(a,b) \in S$ we have
> $$(a,b)\circ(1,0) = (a,b) = (1,0)\circ(a,b).$$

(a,b)-র inverse যদি (c,d) হয় তবে $(ac, bc+d) = (1,0)$ হবে। তার মানে $ac = 1$ এবং $bc + d = 0$ হতে হবে। Solve করে পাই $c = 1/a$ আর $d = -b/a$. এখানেই আমরা ব্যবহার করলাম $a \neq 0$.

> Inverse:
> Shall show that for any $(a,b) \in S$ the inverse is $(1/a, -b/a)$.

তার মানে আমাদের দুটো জিনিস দেখাতে হবে, প্রথমতঃ, $(1/a, -b/a)$ যে আদৌ S-এর মধ্যে আছে সেটা, এবং দ্বিতীয়তঃ, (a,b)-কে এটা দিয়ে গুণ করলে যে identity পাওয়া যায়।

> $(1/a, -b/a) \in S$, since $a \neq 0 \implies 1/a \neq 0$.
> Also,
> $$(a,b)\circ(1/a, -b/a) = (1,0) = (1/a, -b/a)\circ(a,b).$$
> So $(1/a, -b/a)$ is the inverse of (a,b).

এবার দ্বিতীয় অংশ। যদি যে কোনো $(a,b),(c,d) \in S$ নিই, তবে $(a,b)\circ(c,d) = (ac, bc+d)$ কিন্তু $(c,d)\circ(a,b) = (ca, da+b)$. সুতরাং commutative হওয়ার খুব একটা আশা নেই। এটাই একটা counterexample নিয়ে দেখাব--

> No, the group is not commutative, because for
> $$(1,2),(3,4) \in S$$
> we have
> $$(1,2)\circ(3,4) = (3,10),$$
> but
> $$(3,4)\circ(1,2) = (3,6) \neq (1,2)\circ(3,4).$$

■

Example 31: Show that the set G of all ordered pairs (a,b) where a and b are real numbers

and $a \neq 0$ forms a group under the operation $\star$ defined by

$$(a, b) \star (c, d) = (ac, bc + d).$$

Is the group commutative? Justify your answers.[4+1] **(2012.17)**

SOLUTION: আগের অংকটাই। ■

Example 32: Prove or disprove: The set D of all odd integers forms a commutative group with respect to the binary operation '$\star$' defined by

$$a \star b = a + b - 1$$

for $a, b \in D$.[3] **(2009.3bi)**

SOLUTION:

The statement is true.

Closure: To show

$\forall a, b \in D \quad a \star b \in D.$

$\forall a, b$ Take any $a, b \in D$.

Then $a = 2m - 1$ and $2n - 1$ for some $m, n \in \mathbb{Z}$.

So $a \star b = a + b - 1 = 2m - 1 + 2n - 1 - 1 = 2(m + n) - 3$, which is odd, as $m + n \in \mathbb{Z}$. Hence $a \star b \in D$, as required.

Associative: To show

$\forall a, b, c \in D \quad (a \star b) \star c = a \star (b \star c).$

$\forall a, b, c$ Take any $a, b, c \in D$.

Then

$$\begin{aligned}(a \star b) \star c &= (a + b - 1) + c - 1\\ &= a + b + (-1) + c + (-1)\\ &= a + b + c - 2\end{aligned}$$

Similarly, $a \star (b \star c) = a + b + c - 2$.

Hence $(a \star b) \star c = a \star (b \star c)$, as required.

Identity: Shall show 1 is the identity, ie,

$\forall a \in D \quad a \star 1 = 1 \star a = a.$

$\forall a$ Take any $a \in D$.

Then

$$a \star 1 = a + 1 - 1 = a,$$

and

$$1 \star a = 1 + a - 1 = a,$$

as required.

<u>Inverse:</u> Shall show that

$$\forall a \in D \quad \exists b \in D \quad a \star b = b \star a = 1.$$

$\forall a$ Take any $a \in D$.

Then $\because a$ is odd, $\therefore 2 - a$ is an odd integer.

$\exists b$ Choose $b = 2 - a \in D$.

Then

$$\begin{aligned} a \star b &= a + b - 1 = a + 2 - a - 1 = 1, \\ b \star a &= b + a - 1 = 2 - a + a - 1 = 1, \end{aligned}$$

as required.

<u>Commutative:</u> $\forall a, b \in D$

$$a \star b = a + b - 1 = b + a - 1 = b \star a.$$

■

একইরকম আরেকটা অংক তোমার নিজের করার জন্য।

Exercise 20: Let $G = \{3n+1 \ : \ n \in \mathbb{Z}\}$. Consider the binary operation $a \star b = a + b - 1$. Is it true that $(G, \star)$ is an Abelian group? ■

Example 33: Let P be the set of all real numbers except the integer 1. Let the operation '$\star$' in P be defined by

$$a \star b = a + b - ab$$

for all $a, b \in P$. Show that $(P, \star)$ is a group.[3] **(2011.17i)**

SOLUTION: এটা পুরো করে দেব না। খালি লক্ষ কর যে, e যদি identity হয়, তবে সব $a \in P$-এর জন্যই $a \star e = a$ হবে, মানে $a + e - ae = a$ হতে হবে। সুতরাং e কত হবে নিশ্চয়ই বুঝতে পারছ। ■

Exercise 21: আমরা জানি যে $(\mathbb{Z}, +)$ একটা group. এবার আমি '+'-টাকে সামান্য বদলে একটা নতুন binary operation বানাব--

$$a \star b = a + b - 5.$$

তাহলে $(\mathbb{Z}, \star)$ কি একটা group হবে? এখানে 5-এর জায়গায় অন্য সংখ্যা বসালে কী হত? মানে, এমন কী কী $n \in \mathbb{Z}$ আছে যাতে

$$a \star b = a + b - n$$

নিলে $(\mathbb{Z}, \star)$ একটা group হয়? ■

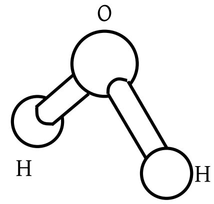


Fig 30

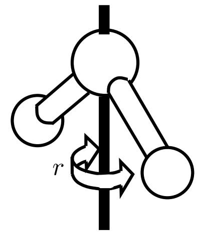


Fig 31

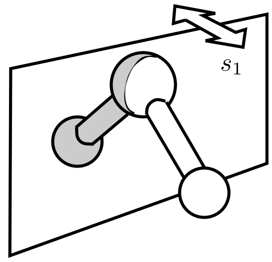


Fig 32

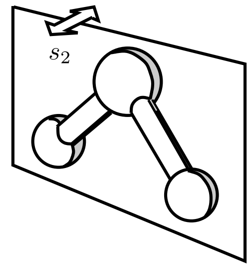


Fig 33

14.1 Group of symmetry

রামগরুড়ের ছানা
হাসতে তাদের মানা।
হাসির কথা শুনলে বলে--
"হাসব? না, না, না, না!"

--সুকুমার রায়

বিশ্বে যতরকমের দরকারী group আছে তাদের মধ্যে অন্যতম হল group of symmetry. জিনিসটা শুধু কাজের তাই নয়, আমার তো বেশ মজাদারও লাগে। তোমাদেরও হয়তো মজা লাগবে এই আশাতেই আজকের আলোচনাটা করছি। তবে যারা নিতান্তই পরীক্ষাপাশের জন্য বইটা পড়ছ, হাতে মজা করার একটুও সময় নেই, তারা বরং আজকের পড়াটা পরীক্ষা শেষের অপেক্ষায় মুলতুবি রেখো। তাতে পরীক্ষা পাশ আটকাবে না!

ধরো কোনো একটা জিনিস আছে, একটা কার্ডবোর্ডের ত্রিভুজ, একটা বই, বা একটা ছক্কা, বা একটা চিনির দানা। মোট কথা শক্তপোক্ত কোনো জিনিস যেটা খানিকটা জায়গা দখল করে থাকে, এবং যেটাকে নাড়াচাড়া করা যায়। সেই জিনিসটাকে নিয়ে যতভাবে ঘুরিয়ে ফিরিয়ে ফের গোড়ার অবস্থানের সঙ্গে ফিট্ করে বসানো যায়, সেইসব নিয়ে সর্বদা একটা group হয়, যাকে বলে ওই জিনিসটার **group of symmetry**. একটা উদাহরণ না দিলে কথাটা গোলমেলে শোনাতে পারে।

Example 34: এই অধ্যায়ের গোড়ায় আমরা যে ত্রিভুজের উদাহরণটা করেছিলাম মনে আছে? ত্রিভুজটা প্রথমে ফ্রেমে ফিট্ করে বসানো ছিল, আমাদের কাজ ছিল সেটাকে ফ্রেম থেকে তুলে আবার ফ্রেমে ফিট্ করে বসানো। আমরা দেখেছিলাম যে ওল্টানো, ঘোরানো ইত্যাদি মিলিয়ে কাজটা মোট 6 ভাবে করা যায়, যাদের নাম দিয়েছিলাম--

$$e, \quad r, \quad \ell, \quad f_1, \quad f_2, \quad f_3.$$

এই 6-জন মিলে একটা group হয়! Binary operation-টা কি সেটা তো আগেই বলেছি। যেমন $f_1 r$ মানে হল প্রথমে ত্রিভুজটাকে তুলে এক ঘর ডানদিকে ঘোরানো (r), এবং তার পর ফ্রেমের 1 নম্বরের প্রান্তটাকে স্থির রেখে ত্রিভুজটাকে উল্টে দেওয়া (f). এর ফলে আমরা পাই $f_1 r = f_2$. ■

কিন্তু এই ছয়জন মিলে খামোখা একটা group হচ্ছে কেন, তার বিস্তারিত আলোচনায় যাব না। খালি এটাই বলব যে, এখানে ত্রিভুজ না হয়ে অন্য যাই হোক না কেন, ফিট্ করে বসানোর সব রকম পদ্ধতি মিলে একটা group হতে বাধ্য।

যাঁরা chemistry নিয়ে গবেষণা করেন, বা যে সব geologist-কে পাহাড়-পর্বতের গা থেকে কুড়িয়ে পাওয়া mineral (খনিজ পদার্থ) চিনতে হয়, group of symmetry তাঁদের খুব কাজে আসে। তোমরা জানো যে, যে কোনো পদার্থই molecule (অণু) দিয়ে তৈরী, আর molecule-গুলো তৈরী atom (পরমাণু) জুড়ে জুড়ে। আমরা যে নুনের দানা দেখি তার একেকটার মধ্যে অনেকগুলো করে molecule থাকে। Molecule-গুলোকে খালি চোখে দেখা যায় না, কিন্তু molecule-এর ভিতরে atom-গুলো কিভাবে সাজানো থাকে তার উপর নির্ভর করে দানাটার আকার, যেটা চোখে দেখে বোঝা যায়। এই যে বললাম "কীভাবে সাজানো থাকে", সেটাকে প্রকাশ করা হয় molecule-টার group of symmetry দিয়ে। একটা উদাহরণ দেখা যাক।

Example 35: Fig 30-এ একটা জলের molecule (অণু) দেখিয়েছি। জল মানে H_2O, দেখতেই পাচ্ছ দুটো H আর একটা O-এর atom নিয়ে তৈরী হয়েছে এটা। এবার আমরা সেই ত্রিভুজের উদাহরণের মত এগোব। Molecule-টাকে তুলে

নিয়ে বিভিন্নভাবে একইজায়গায় ফের ফিট্ করে বসাব। যতভাবে এই কাজটা করা যাবে সেগুলো মিলে একটা group হবে, সেটাই হল molecule-টার group of symmetry.

1. একভাবে তো সবসময়েই বসানো যায়, কিছু না করে। সেটা হল identity, বা e.
2. আরেকটা করা যায় Fig 31-এর মত একটা vertical axis কল্পনা করে সেটা বরাবর $180°$ ঘুরিয়ে দেওয়া। ধরো এর নাম দিলাম r
3. আরেকটা কাজ করা যায়, সেটা হল reflection (প্রতিফলন)। Fig 32-এ যেমন দেখিয়েছি সেইভাবে একটা plane (সমতল) কল্পনা কর। এবার সেই তলে reflection করলেও molecule-টা একই জায়গায় ফিট্ করবে। ধরো এই reflection-টার নামে দিলাম s_1.
4. আরেকভাবেও reflection করা যায়, Fig 33-এর মত করে। সেটার নাম দিলাম s_2.

একটু চিন্তা করলেই দেখবে যে এছাড়া আর কোনোভাবে molecule-টাকে অপরিবর্তিত রাখার উপায় নেই। সুতরাং এই molecule-টার group of symmetry হল $\{e, r, s_1, s_2\}$. ■

এইভাবে বিভিন্ন molecule-এর group of symmetry বার করে তালিকা তৈরী করা আছে। যখন এই molecule-গুলো মিলে কোনো crystal (কেলাস) গঠন করে (যেমন জল জমে বরফ হলে), তখন সেই crystal-গুলোর group of symmetry থেকে molecule-এর group of symmetry বার করা যায়। এবং তা থেকে আন্দাজ করা যায় যে এটা কোন ধরণের molecule থেকে সৃষ্ট।

DAY 15
Equation

Example 36: Let a, b, c be three elements of a group G. Find an element x of G such that $(axb)^{-1} = c^{-1}b^{-1}$. Is such an element unique? Justify your answer.[5] **(1998)**

SOLUTION: এখানে আমাদের একটা সমীকরণের সমাধান করতে হবে-- $a, b, c \in G$ দেওয়া আছে, তা থেকে $x \in G$ বার করতে হবে। এর জন্য একটা সূত্র খেয়াল রাখলে সুবিধা হবে। সেটা হল-- $p, q \in G$ হলে

$$(pq)^{-1} = q^{-1}p^{-1}.$$

লক্ষ কর q^{-1}-টা কিরকম p^{-1}-এর বাঁদিকে চলে গেল। এই অধ্যায়ের গোড়ার দিকে আমরা এই জিনিসটা জুতো-মোজা পরার উদাহরণ দিয়ে শিখেছিলাম। একই ভাবে $p, q, r \in G$ হলে

$$(pqr)^{-1} = r^{-1}q^{-1}p^{-1}.$$

এখানেও p, q, r-এর ক্রম উল্টে গিয়েছে। এ সূত্রটা শুধু দুটো কি তিনটে নয়, যতগুলো খুশী জিনিসের গুণফলের inverse-এর ক্ষেত্রেও প্রযোজ্য। এবার আমাদের অংকটায় ফিরে আসা যাক। দেওয়া আছে--

Given

$$(axb)^{-1} = c^{-1}b^{-1}.$$

আমাদের সূত্রটা লাগিয়ে পাই

> Hence
> $$b^{-1}x^{-1}a^{-1} = c^{-1}b^{-1},$$
> because $(axb)^{-1} = b^{-1}x^{-1}a^{-1}$.

এই বার ছোটোবেলায় যেমন করে সমীকরণের সমাধান করতাম, সব x-কে বাঁদিকে নিয়ে এসে। এর জন্য x ছাড়া বাকী জিনিসগুলোকে ডান দিকে নিয়ে যেতে হবে, এবং বাঁদিক থেকে ডান দিকে যাবার সময়ে তারা যথারীতি উল্টে যাবে। এই ম্যাজিকের পিছনে কারণটা হল inverse দিয়ে গুণ করা। যেমন ধরো এখানে LHS-এর x-এর বাঁদিকে b^{-1} আছে, সেটাকে ডানদিকে নিয়ে যেতে চাই। তার জন্য "ম্যাজিক" কায়দাটা হল--

> b^{-1}-টা LHS থেকে RHS-এ যাবার সময়ে উল্টে b হয়ে যাবে।

এর পিছনের ব্যাখ্যাটা হল--

> আমরা LHS আর RHS দু দিককেই বাঁদিক থেকে b দিয়ে গুণ করছি।

> Multiplying both sides by b from the left,
> $$bb^{-1}x^{-1}a^{-1} = bc^{-1}b^{-1},$$
> or,
> $$x^{-1}a^{-1} = bc^{-1}b^{-1},$$

এবার ডানদিকের a^{-1}-টার পালা--

> Similarly, multiplying both sides by a from the right,
> $$x^{-1}a^{-1}a = bc^{-1}b^{-1}a,$$
> or
> $$x^{-1} = bc^{-1}b^{-1}a.$$

এবার এই x^{-1}-টাকে উল্টে x বানাতে হবে। এখানে আমরা এই সূত্রটা লাগাচ্ছি যে কারো inverse-এর inverse হচ্ছে সে নিজেই!

> So, inverting both sides,
> $$x = \left(x^{-1}\right)^{-1} = (bc^{-1}b^{-1}a)^{-1}.$$

ডান দিকে চারটে জিনিসের গুণফলের inverse রয়েছে। আমরা গুণফলের inverse বার করার সূত্র তো জানিই, ক্রমটাকে উল্টে সবাইকে আলাদা আলাদা করে inverse করে দেওয়া--

> Hence
> $$x = a^{-1}bcb^{-1},$$
> which is the required answer.

এবার জিজ্ঞাসা করেছে "Is such an element unique?" অর্থাৎ আমরা যে x-টা পেলাম তা ছাড়াও আরও x আছে কিনা যার জন্য $(axb)^{-1} = c^{-1}b^{-1}$ হয়। উত্তর হচ্ছে, "না নেই, কারণ আমরা এই equation থেকে ধাপে ধাপে কষে যাওয়াতেই x-এর এই একমাত্র value-টা বেরিয়েছে।"

> As the above steps show
> $$(axb)^{-1} = c^{-1}b^{-1} \implies x = a^{-1}bcb^{-1}.$$
> So the solution is unique.

চাইলে আমরা uniqueness-টা আরেকভাবেও দেখাতে পারতাম। তার জন্য ধরো x_1, x_2 দুজনেই প্রশ্নে দেওয়া equation-টাকে satisfy করে, অর্থাৎ--
$$(ax_1b)^{-1} = c^{-1}b^{-1} \text{ এবং } (ax_2b)^{-1} = c^{-1}b^{-1}.$$
এথেকে আমরা দেখাতে পারব যে $x_1 = x_2$. সেটা এইভাবে--এই দুটো equation-এর RHS-এ একই জিনিস আছে। অতএব $(ax_1b)^{-1} = (ax_2b)^{-1}$.
দু পাশের inverse নিলে, $ax_1b = ax_2b$. এবার বাঁদিক থেকে a আর ডানদিক থেকে b কেটে নিলেই $x_1 = x_2$ পেয়ে যাবে। ■

এইবার যে অংকটা করব, সেটা নিছক কসরতের। Group theory শেখার জন্য এদের প্রয়োজন সামান্যই। পরীক্ষাপাশের ভূত মাথায় না থাকলে এই অংকটা স্বচ্ছন্দে বাদ দিয়ে যেতে পারো।

Example 37: Let $(G, \star)$ be a group and $a, b \in G$. Suppose that $a^2 = e$ and $a \star b \star a = b^7$. Prove that $b^{48} = e$, where e is the identity element of G.[3] **(2009,2013)**

SOLUTION:

> We have $a \star b \star a = b^7$. Raising to the 7-th power,
> $$(a \star b \star a)^7 = (b^7)^7 = b^{49}.$$
> Now, using associativity,
> $$\begin{aligned}(a \star b \star a)^7 &= \underbrace{\underbrace{a \star b \star a} \star \cdots \star \underbrace{a \star b \star a}}_{7 \text{ times}} \\ &= a \star b^7 \star a \quad [\because a^2 = e] \\ &= a \star a \star b \star a \star a \quad [\because a \star b \star a = b^7] \\ &= b \quad [\because a^2 a = e]\,.\end{aligned}$$

লক্ষ কর কীভাবে এখানে শুরুতেই "using associativity" লিখেছি। আসলে প্রায় প্রতি ধাপেই একবার করে associativity লাগে, তাই একেবারে গোড়াতেই কৃতজ্ঞতা স্বীকার করে নিয়েছি। বার বার করে প্রতি ধাপে লিখতে হাত ব্যথা হয়ে যেত।

> Hence
> $$b = b^{49}.$$
> Cancelling b from both sides
> $$b^{48} = e,$$
> as required.

■

15.1 Abelian দেখানো

এবার আমরা কিছু অংক দেখব যেখানে একটা group-এর উপর কিছু শর্ত দেওয়া থাকবে, এবং তা থেকে দেখাতে হবে যে, group-টা Abelian. এই অংকগুলো নিছক কসরৎ ছাড়া আর কিছুই নয়, group theory শেখায় এদের গুরুত্ব নেই বললেই হয়।

Example 38: In a group G if $a = a^{-1}$ for all $a \in G$, then prove that G is a commutative group. Is the converse true? Justify your answer.[3] **(1997,2001,2005)**

SOLUTION:

> Given: G is a group with
> $$\forall a \in G \quad a = a^{-1}.$$
> To show: G is commutative, ie,
>
> $\forall p, q \in G \quad pq = qp.$
>
> $\forall p, q$
>
> Take any $p, q \in G$.
>
> Then by the given condition,
> $$pq = (pq)^{-1},$$

যেহেতু এই group-এ সবাই নিজের নিজের inverse.

> or,
> $$pq = q^{-1}p^{-1},$$
> or, since $p = p^{-1}$ and $q = q^{-1}$ by the given condition,
> $$pq = qp,$$
> as required.

দ্বিতীয় অংশে converse নিয়ে কাজ করতে বলেছে। সেটা কী হবে বুঝে নিই। মূল statement-টা ছিল--

"$\big(\forall a \in G \quad a^{-1} = a\big) \implies G$ is commutative."

কোনো $\implies$-জাতীয় statement-এর converse পাওয়া যায় $\implies$-এর দুই দিকের স্থান বিনিময় করলে, মানে এক্ষেত্রে converse-টা হবে--

> The converse is
>
> "G is commutative $\implies \big(\forall a \in G \quad a^{-1} = a\big)$."
>
> No, the converse is not true. Consider $(\mathbb{Z}, +)$, which is commutative with $n^{-1} = -n$. But we know that $-1 \neq 1$.

■

Example 39: True or false: In a group $(G, \bullet)$ if $(a \bullet b)^2 = a^2 \bullet b^2$ for all $a, b \in G$ then $(G, \bullet)$ is Abelian.[2] **(2000)**

SOLUTION:

Given: $\forall a, b \in G \quad (a \bullet b)^2 = a^2 \bullet b^2$, or $a \bullet b \bullet a \bullet b = a^2 \bullet b^2$, or, cancelling a from left and b from right,

$$b \bullet a = a \bullet b.$$

Hence $(G, \bullet)$ is Abelian.
So the statement is true.

■

Example 40: Prove that a group is commutative if and only if $(ab)^{-1} = a^{-1}b^{-1}$ for all $a, b \in G$.[5] **(1998)**

SOLUTION:

``Only if" part: Given G is commutative.

To show

$\forall a, b \in G \quad (ab)^{-1} = a^{-1}b^{-1}$.

$\forall a, b$ Take any $a, b \in G$.

Then

$$(ab)^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1} \quad [\because G \text{ is commutative}],$$

as required.

এবার অন্য দিকটা--

"If" part: Given: $\forall a, b \in G \quad (ab)^{-1} = a^{-1}b^{-1}$.

To show: G is commutative, ie,

$\forall a, b \in G \quad ab = ba$.

$\forall a, b$ Take any $a, b \in G$.

Then, by the given condition and associativity,

$$
\begin{aligned}
& (ab)^{-1} = a^{-1}b^{-1} \\
\text{or,}\quad & (ab)(a^{-1}b^{-1}) = e, \\
\text{or,}\quad & (aba^{-1})b^{-1} = e, \\
\text{or,}\quad & aba^{-1} = b, \quad \left[\text{multiplying by } b \text{ from right.}\right] \\
\text{or,}\quad & ab = ba \quad \left[\text{multiplying by } a \text{ from right.}\right],
\end{aligned}
$$

as required.

■

Exercise 22: True or false: A group G is Abelian if $b^{-1}a^{-1}ba = e$, where $a, b \in G$ and e is the identity element of G.[2] **(2002)**

HINT:

এটা বস্তুতঃ আগের অংকের if অংশটার রূপান্তর। এখানে বলে দিয়েছে $b^{-1}a^{-1}ba = e$, তার মানে ba-র সঙ্গে $b^{-1}a^{-1}$ গুণ করলে e পাওয়া যায়। অতএব $(ba)^{-1} = b^{-1}a^{-1}$, ঠিক যেমনটা আগের অংকে দেওয়া ছিল (খালি এখানকার a ওখানে ছিল b, আর এখানকার b-টা ছিল ওখানকার a). ■

Example 41: Let G be a group. If $a^{-1}b^2(bab)^{-1}ba^2 = b$ for all $a, b \in G$, then show that G is a commutative group. **(2003)**

SOLUTION:

To show

$\forall a, b \in G \quad ab = ba.$

$\forall a, b$ Take any $a, b \in G$.

এইবার বার বার associativity লাগাতে হবে--

By the given condition and associativity,

$$
\begin{aligned}
& a^{-1}b^2(bab)^{-1}ba^2 = b \\
\text{or,}\quad & b^2(bab)^{-1}ba^2 = ab \quad \left[\text{multiplying by } a \text{ from left.}\right] \\
\text{or,}\quad & b^2b^{-1}a^{-1}b^{-1}ba^2 = ab \quad [\because (bab)^{-1} = b^{-1}a^{-1}b^{-1}.] \\
\text{or,}\quad & ba^{-1}a^2 = ab \\
\text{or,}\quad & ba = ab,
\end{aligned}
$$

as required.

■

Example 42: True or false: Let G be a group. For all $x, y, z \in G$ if $xy = yz$ then $x = z$. Then G is an Abelian group.[2] **(2003)**

SOLUTION: এখানে কী চেয়েছে বুঝে নিই। একটা group দেওয়া আছে G, যার জন্য $xy = yz$ হলেই $x = z$ হয় (ঠিক যেন y-টা কাটাকাটি হয়ে গেল, যদিও ওটা LHS-এ আছে ডানপাশে, আর RHS-এ বাঁপাশে)। জানতে চেয়েছে--এরকম G কী Abelian হতে বাধ্য?

> To check if
> $$\forall a, b \in G \quad ab = ba.$$

শুরুটা যথারীতি--

> Take any $a, b \in G$.

বলা আছে যে $xy = yz$ হলে $x = z$ হয়। আমরা করব কি, $x = ab$ আর $z = ba$ নেব। তাহলে $x = z$ মানে হবে $ab = ba$.

> Let $x = ab$ and $z = ba$.

এবার $x = z$ পেতে হলে দরকার $xy = yz$. তাই এমন একটা y নেব যাতে তা হয়, অর্থাৎ $aby = yba$ হয়। একটু ভাবলেই মাথায় আসে যে, $y = b^{-1}$ নিলেই b-টার সাথে কাটাকাটি হয়ে গিয়ে দুদিকেই খালি a পড়ে থাকবে।

> Let $y = b^{-1}$.
> Then
> $$xy = (ab)b^{-1} = a(bb^{-1}) = ae = a,$$
> and also
> $$yz = b^{-1}(ba) = (b^{-1}b)a = ea = a.$$

সুতরাং $xy = yz$ পেয়ে গিয়েছি। তাই--

> So $xy = yz$, and hence by the given condition $x = z$, or
> $$ab = ba.$$

এই বার একটা উপসংহার টানা যাক--

> Since $a, b \in G$ was arbitrary, this shows that G is Abelian.
> So the statement is true.

■

Example 43: If G is a group in which $(ab)^3 = a^3b^3$ and $(ab)^5 = a^5b^5$ for all $a, b \in G$, prove that G is Abelian.[3] **(2006)**

SOLUTION: এই অংকটা একটু কঠিন। কয়েকবার এদিক ওদিক ঢুঁ না মারলে বোঝা শক্ত কী করে এগোব। অবশ্য প্রমাণের শুরুটা এমনি যেমন হয় সে রকমই--

To show
$\forall a, b \in G \;\; ab = ba.$
$\forall a, b$ Take any $a, b \in G$.

দুটো সমীকরণ দেওয়া আছে। তার মধ্যে প্রথমটা হল--

Now $(ab)^3 = a^3b^3$,

বড় করে লিখলে হয়--

or, $ababab = aaabbb$,

বাঁপাশ থেকে একটা করে a আর ডানপাশ থেকে একটা করে b কাটার সুবর্ণ সুযোগ।

or, left cancelling a and right cancelling b,

$$baba = aabb. \quad (*)$$

আর কিছু কাটা যাচ্ছে না। সুতরাং এটা আপাততঃ এখানেই থাক, আমরা অন্য সমীকরণটাকে নিয়ে পড়ি--

Also, $(ab)^5 = a^5b^5$,
or, $ababababab = aaaaabbbbb$,

আবার কাটাকাটির সুযোগ--

or, left cancelling a and right cancelling b,

$$babababa = aaaabbbb$$

আর কিছুই কাটাকাটি যাচ্ছে না। কিন্তু বাঁদিকে আছে দুটো $baba$. আমরা (*) থেকে জানি যে $baba = aabb$. সুতরাং $baba$-দের জায়গায় $aabb$ বসিয়ে পাই--

or, by (*),

$$aabbaabb = aaaabbbb.$$

আবার কাটা যাবে! বাঁপাশ থেকে দুটো a আর ডানপাশ থেকে দুটো b.

or, cancelling aa from left and bb from right, $bbaa = aabb$,

অনেকটা ছোটো হল বটে, কিন্তু এখনো $ab = ba$-তে পৌঁছোয় নি। মানে আরো কাটা দরকার। তার জন্যে দুই দিকেরই একই পাশে একই অক্ষর চাই। আরেকবার (*) লাগালে ডান দিকের $aabb$-টা $baba$ বানানো যাবে--

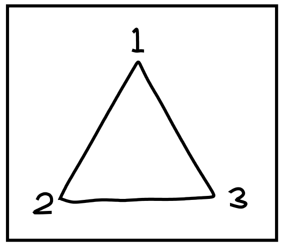


Fig 34

> or, using (*), $bbaa = baba$,

এবং তার মানেই আবার কাটাকাটি--

> or, left cancelling b and right cancelling a,
>
> $$ba = ab,$$
>
> as required.

■

মনে কর G একটা Abelian group, আর $a, b \in G$. তবে বুঝতেই পারছ যে $baba = abba$, অর্থাৎ বাবা = আব্বা। সত্যিই তো হিন্দুরা যাকে বাবা ডাকে, মুসলমানেরা তো তাকেই আব্বা বলে। "ধর্মসমন্বয়ে group theory-র প্রয়োগ" নিয়ে কেউ যে কেন গবেষণা করে না কে জানে! তাহলে বিভিন্ন ধর্মের মানুষ কেমন সংকীর্ণ দলের চিন্তা ভুলে group-এর চিন্তায় মেতে উঠত!

DAY 16
Order (part 1)

এইবার আমরা যে অংকগুলো করব, সেখানে বার বার করে একটা শব্দ ব্যবহৃত হবে-- **order**. এই শব্দটার দুটো অর্থ আছে, কখন কোন অর্থে ব্যবহৃত হচ্ছে, সেটা পড়বার সময়ে বুঝে নিতে হবে--

- যখন লেখে "G is a group of order 5" তার মানে G group-টার সাইজ 5, অর্থাৎ G ঠিক 5-টা element নিয়ে তৈরী।
- যদি লেখে "$a \in G$ has order 5" তার মানে কিন্তু সম্পূর্ণ অন্য। এর মানে হল--a-র power যদি আমরা $a, a^2, a^3, \ldots$ এইভাবে বাড়াতে থাকি, তবে প্রথম যে power-টা identity-র সমান হবে সেটা হল a^5, অর্থাৎ

$$a, a^2, a^3, a^4 \neq e \text{ কিন্তু } a^5 = e.$$

একটা উদাহরণ নিই।

Example 44: ধরো সৈনিকের প্যারেডের উদাহরণটা। সেখানে group-টা ছিল

{হল্ট, বাঁয়, পিছে, ডাইনে}.

এর মধ্যে identity ছিল "হল্ট"। আমরা বার করতে চাই "বাঁয়"-র order কত।
SOLUTION: এর জন্য আমরা সৈনিকটাকে বার বার করে "বাঁয় মুড়" বলতে থাকব। প্রথমবার বলার পর সৈনিকটা একঘর বাঁদিকে ঘুরবে, দ্বিতীয়বারের পর পিছনে, তৃতীয়বারের পর ডানদিকে, এবং চতুর্থবারের পর ফের শুরুর দিকে মুখ করে দাঁড়াবে। সুতরাং "বাঁয়"-র order হল 4. ■

একই যুক্তিতে "পিছে"-র order হবে 2, কারণ একবার "পিছে" বললে সৈনিকটা পিছনে ফিরবে এবং দুইবার বললে ফের গোড়ার অবস্থানে ফিরে যাবে।

Exercise 23: বল তো "ডাইনে"-র order কত হবে। আর "হল্ট"-এর order-ই বা কত? ■

Exercise 24: আবার সমবাহু ত্রিভুজের উদাহরণটা দেখা যাক (Fig 34)। সেখানে r মানে ছিল ত্রিভুজটাকে ডানদিকে $120°$ ঘোরানো। বলতে হবে r-এর order কত। ■

এবার তবে সংজ্ঞাটা লিখে ফেলি।

DEFINITION: **Order of a group element**

If G is a group and $a \in G$, then the **order** of a is defined as the least $n \in \mathbb{N}$ such that $a^n = e$, where e is the identity element of G. It is denoted by $o(a)$. If no such $n \in \mathbb{N}$ exists then we say $o(a) = \infty$.

এখানে ∞-র ব্যাপারটা একটা উদাহরণ দিয়ে বুঝে নিই।

Example 45: ধরো আমাদের group-টা হল $(\mathbb{Z}, +)$. তাহলে 1-এর order কত?

SOLUTION: এখানে identity হল 0. আমরা $1 + 1 + \cdots$ এইভাবে যোগ করতে থাকব, এবং দেখব কখন যোগফলটা 0 হয়। পর পর বার করতে থাকি--

$$\begin{aligned} 1 &\neq 0 \\ 1+1 &\neq 0 \\ 1+1+1 &\neq 0 \\ &\vdots \end{aligned}$$

বুঝতেই পারছ যে, এভাবে এগোলে কোনোদিনই 0 পাওয়া যাবে না। তাই বলব $o(1) = \infty$. ■

Exercise 25: $(\mathbb{Z}, +)$-এর সব element-এরই order হল ∞, খালি একজন বাদে। সেই ব্যতিক্রমটি কে? তার order কত? ■

যদি বলে--

"a has order 5"

তবে তার কয়েকটা ফলশ্রুতি আছে যেগুলো একে একে আলোচনা করব। এখানে 5-এর আলাদা কোনো গুরুত্ব নেই, অন্য যেকোনো finite সংখ্যা থাকলেও একইরকম ব্যাপার হত।
প্রথম ফলশ্রুতি হল--

1 a-র যেকোনো power-ই এই 5-টা power-এর কোনোটার সমান হবে--

$$a^0, a, a^2, a^3 \text{ আর } a^4.$$

এখানে $a^0 = e$.

যেমন $a^6 = a^5 a = ea = a$. একইভাবে $a^{13} = a^{2\times5+3} = (a^5)^2 a^3 = e^2 a^3 = a^3$. একইরকম ব্যাপার negative power-দের ক্ষেত্রেও, যেমন $a^{-1} = a^4$. কারণ $aa^4 = a^4 a = a^5 = e$. যদি তোমাকে একটা power a^n দেওয়া হয়, তাহলে তুমি n-কে 5 দিয়ে ভাগ করে ভাগশেষ নাও, যদি ভাগশেষটা হয় r, তবে $a^n = a^r$ হবে।

2 a-এর প্রথম পাঁচটা power (মানে a^0, a, a^2, a^3, a^4) কেউ কারো সমান হতে পারবে না।

যদি ধরো $a^2 = a^4$ হত, তবে দুদিক থেকে a^2 কেটে পেতাম $e = a^2$, কিন্তু তা তো হতে পারে না, কারণ a^5-এর থেকে ছোটো কোনো power তো identity-র সমান নয়!

3 $a^n = e \iff 5|n$, অর্থাৎ $a^n = e$ হবে একমাত্র তখনই যখন n সংখ্যাটা 5 দিয়ে ভাগ যাবে।

যেমন $a^{99} = e$ হতে পারে না, কারণ 99-কে 5 দিয়ে ভাগ করলে ভাগশেষ হয় 4. তাই $a^{99} = a^4 \neq e$, কারণ a^5-এর চেয়ে ছোটো কোনো positive power তো e হতে পারে না। এই ব্যাপারটাকে অন্যদিক দিয়ে দেখা যায়--

Example 46: ধরো $b \in G$ এমন একটা element যার জন্য $b^{15} = e$. তাহলে b-এর order সম্পর্কে কী সিদ্ধান্ত করা যায়?

SOLUTION: এখানে b-এর order অবশ্যই 15-র একটা factor (অর্থাৎ গুণনীয়ক) হতে বাধ্য। তার মানে order-টা হবে হয় 1 বা 3 বা 5 বা 15. ■

আরো একটা কথা মনে রেখো--

THEOREM

যে কোনো group-এ কেবল একটাই element আছে যার order 1. সেটা হল identity.

সবশেষে একটা গুরুত্বপূর্ণ জিনিস বলে রাখি, যেটা আমরা পরের অধ্যায়ে শিখব, যখন Lagrange's theorem (লাগ্রাঞ্জের থিওরেম) আলোচনা করা হবে। কিন্তু ব্যাপারটা এখন থেকেই মাথায় রাখা ভালো, যদিও এটা আমরা এই অধ্যায়ের কোনো অংকে ব্যবহার করব না।

> ধর G হল একটা finite group, যার সাইজ n. এই group-টার যেকোনো একটা element নাও $g \in G$. তাহলে g-এর order দিয়ে n ভাগ যেতে বাধ্য! মানে element-এর order দিয়ে group-এর order-টা ভাগ যাবেই।

যেমন ধর G-এর সাইজ যদি হত 10, তবে তার মধ্যে কোনো ভাবেই এমন কোনো element থাকতে পারে না, যার order হল 3, কারণ 3 দিয়ে 10-কে ভাগ যায় না।
এইবার কয়েকটা সহজ অংক করি। এদের প্রতি ক্ষেত্রেই তোমাকে কোনো একটা element-এর order বার করতে হবে। তোমার কাজ হবে $a, a^2, a^3, \ldots$ বার করে যাওয়া, এবং দেখা কখন প্রথম $a^n = e$ হয়। সেই n-টাই হবে a-র order.

Example 47: If b is an element of a group and order of b is 20, find the order of b^{15}.[2] **(2010.3bii)**

SOLUTION:

> Let $a = b^{15}$.

আমরা $o(a)$ বার করতে চাই, তার মানে $a, a^2, a^3, \ldots$ ইত্যাদি বার করে যাব, এবং দেখব কখন e পাই। a-এর power-রা আবার b-এরও power, যেমন $a = b^{15}$, $a^2 = b^{30}$, ইত্যাদি। সুতরাং আগে দেখে রাখি b-এর power-রা কখন e-এর সমান হয়।

> Since $o(b) = 20$ hence $b^n = e$ iff $20|n$.
> So $a = b^{15} \neq e$, since $20 \nmid 15$,

এখানে $20 \nmid 15$ মানে "20 দিয়ে 15-কে ভাগ যায় না"।

> and $a^2 = b^{30} \neq e$, since $20 \nmid 30$,
> and $a^3 = b^{45} \neq e$, since $20 \nmid 45$.
> But $a^4 = b^{60} = e$, since $20|60$.
> So $o(a) = 4$.

■

একই রকম আরও দুটো অংক দিলাম নীচে, নিজে নিজে করার জন্য।

Exercise 26: Let G be a group and $a \in G$. If $o(a) = 24$ find $o(a^4)$.[2] **(2012.16i)** ■

Exercise 27: Let a be an element of order 16 in a multiplicative group. Find the order of a^3.[2] **(2008)**
HINT: এখানে আলাদা করে "multiplicative" কথাটার বিশেষ কোনো মূল্য নেই। ওর অর্থ হল binary operation-টাকে গুণের মত লেখা হবে। ■

এই দুটো অংকের মধ্যে একটা প্যাটার্ণ দেখতে পাচ্ছ? দুইক্ষেত্রেই $o(a)$ বলে দিয়ে a-র কোনো একটা power-এর order জানতে চাওয়া হয়েছিল। ধরো $o(a) = m$ আর বার করতে বলেছে $b = a^n$-এর order. তাহলে আমরা b-এর পরপর power-গুলো নিয়ে পরীক্ষা করছি, প্রথম কখন e পাই। তার মানে সবচেয়ে ছোটো $k \in \mathbb{N}$ খুঁজছি যাতে $b^k = e$ হয়। কিন্তু $b^k = a^{nk}$, এবং সেটা e-এর সমান হবে যদি $m|nk$ হয় (কারণ $o(a) = m$)। সুতরাং nk-টা একইসঙ্গে n-এরও multiple (গুণিতক) এবং m-এরও multiple হতে হবে, এবং $k \in \mathbb{N}$-কে যথাসম্ভব ছোটোও হতে হবে। সুতরাং বুঝতেই পারছ যে, kn হবে m এবং n-এর LCM (লসাগু)। এইটাকে একটা ছোট্টো theorem হিসেবে লিখে ফেলা যাক--

THEOREM

Let G be a group. Let $a \in G$ with $o(a) = m$. Then for any $n \in \mathbb{N}$

$$o(a^n) = LCM(m, n)/n.$$

এবার এই theorem-টা দিয়ে নীচের অংকটা কর দেখি।

Exercise 28: If G is a group and $a \in G$ has $o(a) = 101$, then find $o(a^{35})$. ■

এই কায়দায় আমরা $o(a)$ জানলেই যে কোনো $n \in \mathbb{N}$-এর জন্যই $o(a^n)$ বার করে ফেলতে পারি। কিন্তু যদি n শূন্য বা negative হয়? যদি $n = 0$ হয় তবে a^0-কে define-ই করা হয় $a^0 = e$ হিসেবে, সুতরাং $o(a^0) = 1$. আর যদি $n < 0$ হয় তবে নীচের theorem-টা কাজে দেবে।

THEOREM

Let G be any group. Then for any $a \in G$ we have $o(a^{-1}) = o(a)$.

প্রমাণটা খুবই সহজ--এই কথাটা ব্যবহার কর যে $(a^{-1})^n = (a^n)^{-1} = e \iff a^n = e$.

Example 48: ধরো একটা group আছে, তার একটা element হল a. বলা আছে $o(a) = 10$. তোমাকে বার করতে হবে $o(a^{-4})$ কত।

SOLUTION: লক্ষ করো যে $a^{-4} = (a^4)^{-1}$. সুতরাং উপরের theorem-টা থেকে পাচ্ছ $o(a^{-4}) = o(a^4)$. আর $o(a^4) = LCM(4, 10)/4 = 20/4 = 5$. সুতরাং $o(a^{-4}) = 5$. ■

এবার সামান্য অন্য স্বাদের একটা অংক।

Exercise 29: If, in an Abelian group, $o(a) = 3$ and $o(b) = 5$ then find $o(ab)$.

HINT: $(ab)^{15} = a^{15}b^{15}$, যেহেতু Abelian. সুতরাং $(ab)^{15} = e$. অতএব $o(ab)|15$. তার মানে $o(ab) = 1, 3, 5$ বা 15. প্রশ্ন হল এদের মধ্যে কোন কোন value বাদ যাবে।$o(ab) = 1$ হতে পারে না, তাহলে $b = a^{-1}$, কিন্তু $o(a) \neq o(b)$. আবার $o(ab) = 3$-ও হতে পারে না, কারণ তাহলে $a^3 = e$ হয়ে যাচ্ছে। একইভাবে $o(ab) = 5$ হলে $b^5 = e$ হবে, যেটা অসম্ভব। সুতরাং $o(ab) = 15$-ই হতে হবে। ■

Example 49: Suppose a group contains elements a, b such that $o(a) = 4$, $o(b) = 2$ and $a^3b = ba$.

Find $o(ab)$.[3] **(2014.16b)**

SOLUTION:

Clearly $ab \neq e$.

⟦ Because:

Otherwise, $b = a^{-1}$, and hence $o(a) = o(b)$, which is not true.

⟧

Hence $o(ab) \neq 1$.

$$
\begin{aligned}
abab &= a(ba)b \\
&= a(a^3b)b \quad [\because a^3b = ba] \\
&= a^4b^2 \\
&= ee \quad [\because o(a) = 4, o(b) = 2] \\
&= e.
\end{aligned}
$$

Hence $o(ab) = 2$.

■

16.1 Finite/infinite

আগেই বলেছি যে, group theory-তে order শব্দটা দুটো সম্পূর্ণ আলাদা অর্থে ব্যবহৃত হয়--

- একটা group-এর order মানে হল তার সাইজ, অর্থাৎ group-টায় কতগুলো element আছে।
- একটা element $a \in G$-এর order হল সবচেয়ে ছোটো $n \in \mathbb{N}$ যাতে $a^n = e$ হয়। যদি কোনো $n \in \mathbb{N}$-এর জন্যই $a^n = e$ না হয় তবে $o(a) = \infty$ বলি।

এই দুই ধরণের order-এর মধ্যে ঘনিষ্ঠ সম্পর্ক আছে। যেমন একটা সম্পর্ক হল--যদি group-এর order-টা finite হয়, তবে তার যাবতীয় element-এর order-ও finite হতে বাধ্য! নীচের অংকে এটাই প্রমাণ করতে দিয়েছে।

Example 50: Prove that each element of a finite group is of finite order.[2] **(2006)**

SOLUTION:

Let G be a finite group of order n. Shall show $\forall a \in G \quad o(a) < \infty$.

চট্ করে ভেবে নিই $o(a) < \infty$ মানে কী। এর মানে হল a-র কোনো একটা power পাওয়া যাবে a^k, যেটা e-এর সঙ্গে সমান এবং $k \in \mathbb{N}$. এই কথাটা লিখে নিই--

ie,

◎ $\forall a \in G \quad \exists k \in \mathbb{N} \quad a^k = e.$

প্রমাণের শুরুটা যথারীতি--

$\forall a$ Take any $a \in G$.

আমরা এবার পরপর $a, a^2, a^3, \ldots$ করে a-র power-গুলো নিতে থাকব। যেহেতু G হল finite, সুতরাং এরা তো সবাই আলাদা আলাদা হতে পারে না। বস্তুতঃ প্রথম $n+1$-খানা power নিলেই ওদের মধ্যে অন্ততঃ দুটো এক হতে বাধ্য। ঠিক যেমন অন্ধকারের মধ্যে হাতড়ে যদি তিনটে মোজা নাও, তবে তার মধ্যে দুটো মোজা একই পায়ের হতে বাধ্য, কারণ পা তো মোটে দুটো!

Consider $a, a^2, ..., a^{n+1} \in G$.

Since $|G| = n$, so these $n+1$ elements cannot all be distinct.

Hence $\exists i \neq j \quad a^i = a^j$.

W.l.g., $i < j$.

এখানে w.l.g. মানে হল without loss of generality. এটা কেন লিখলাম বলি--আমরা খালি $i \neq j$ ধরেছিলাম। সুতরাং হয় $i < j$ নয়তো $i > j$. এই দুইক্ষেত্রেই প্রমাণটা একেবারে একই যুক্তিতে এগোবে, তাই যে কোনো একটা কেস করলেই হয়। আমরা এখানে $i < j$ নিয়ে কাজ করব। এতে $i > j$ কেসটা বাদ গেল বটে, কিন্তু যুক্তির দিক দিয়ে কিছু বাদ গেল না। সেই জন্যই লিখেছি without loss of generality, অর্থাৎ একটা কেস বাদ দিলেও আমাদের যুক্তিটা general-ই আছে।

Cancelling a^i from both sides, we get $e = a^{j-i}$.

$\exists k$ Choose $k = j - i \in \mathbb{N}$.

Then $a^k = a^{j-i} = e$, as required.

■

কোনো group-এর order যদি finite হয়, তবে তার সব element-এর order-ও যে finite হবেই সেটা দেখা গেল। এর converse-টা (মানে উল্টোটা)-ও কি ঠিক? অর্থাৎ, কোনো group যদি এমন পাওয়া যায়, যার প্রতিটি element-এর order-ই হল finite, তবে সেই group-টা কি finite হতে বাধ্য? এর উত্তর কিন্তু--না। এরকম একটা counterexample চেয়েছে নীচের অংকটায়।

Example 51: Give an example of an infinite group whose every element is of finite order.[2]

(2009.3bii)

SOLUTION:

Let G be the power set of $\mathbb{N}$, which is a group under the binary operation symmetric difference:

$$A \Delta B = (A \cap B^c) \cup (A^c \cap B).$$

By standard result (G, Δ) is a group with identity ϕ.

Then for every element $A \in G$ we have

$$A \Delta A = \phi.$$

So every element has finite order.

> But since $\mathbb{N}$ is an infinite set, G must also be infinite.

■

এই অংকে যে power set-এর কায়দাটা লাগালাম, সেটা পরের অংকটাতেও লাগবে। যদিও এখানে আমরা finite group নিয়ে কাজ করব।

Example 52: Give an example of a finite group whose each element other than the identity has the same order and also the order of the group is not a prime number.[2] **(2010.3ci)**

SOLUTION:

> Let G be the power set of $\{1,2\}$, which is a group under the binary operation symmetric difference:
>
> $$A\Delta B = (A\cap B^c)\cup(A^c\cap B).$$
>
> By standard result (G,Δ) is a group with identity ϕ.

এই group-টার সঙ্গে আমাদের আগেও মোলাকাত হয়েছে। তখনই বলেছিলাম যে, এর একটা পোশাকী নাম আছে--**Klein's 4-group,** যাকে অনেক সময়ে K_4 চিহ্ন দিয়ে লেখা হয়-- সেই কথাটা এই বেলা উল্লেখ করে দিলে মন্দ হয় না।

> (Actually this is the same as Klein's 4 group (K_4).)
>
> Then for every element $A\in G$ we have
>
> $$A\Delta A = \phi.$$
>
> So every element has order that divides 2.
>
> So all non-identity elements have order 2.
>
> The order of the group is $2^2 = 4$, which is finite and not a prime.

■

DAY 17
Order (part 2)

আজকে আমরা আরো কিছু order-এর অংক করব। এর মধ্যে প্রথম অংকটা আমাদের পূর্বপরিচিত।

Exercise 30: If every element, except identity, of a group is of order 2, show that the group is commutative. Is the converse true? Justify your answer.[2+1] **(2012.16ii,2002.8bi)**

HINT:

এটা আসলে গত পরশুর Example 38-এর অংকটাই। যদি identity ছাড়া অন্য সব a-এর order হয় 2, তবে $a = a^{-1}$ হবেই। আর $a = e$ হলে তো $a = a^{-1}$ হবেই। সুতরাং এবার Example 38-এর সমাধানটা করে গেলেই হবে। ■

এবার একটা জিনিস শিখতে চলেছি, যেটা বেশ গুরুত্বপূর্ণ। নীচের অংকটা গা গরম করার জন্য--

Example 53: In a group G, a, b are distinct elements of order 2. Prove that if a, b do not commute, then $o(aba^{-1}) = 2$.[2] **(2013.17b)**

SOLUTION: এখানে আমরা প্রথম দেখাব $aba^{-1} \neq e$. তারপর দেখাব $\left(aba^{-1}\right) = e$. ব্যস্, তাহলেই হয়ে যাবে!

> Step 1: We have $aba^{-1} \neq e$.
>
> ⟦ Because:
>
> Otherwise, $aba^{-1} = e$, and so $b = a^{-1}a = e$. Then $o(b) = 1 \neq 2$.
>
> ⟧
>
> Step 2: We have
>
> $$\begin{aligned} \left(aba^{-1}\right)^2 &= aba^{-1}aba^{-1} \\ &= ab^2a^{-1} \\ &= aa^{-1} \quad [\because o(b) = 2] \\ &= e. \end{aligned}$$
>
> Thus $o\left(aba^{-1}\right) = 2$, as required.

লক্ষ করো যে, অংকটায় বিস্তর অপ্রয়োজনীয় তথ্য দিয়েছিল, যেমন a, b হল distinct, ওরা commute করে না (মানে $ab \neq ba$) এবং $o(a) = 2$. এগুলোর কোনোটাই কাজে লাগেনি। ■

সুতরাং আমরা যেটা প্রমাণ করলাম সেটা হল-- $o(b) = 2$ হলেই $o\left(aba^{-1}\right) = 2$ হতে বাধ্য। এবং সেটা প্রমাণ করা গেল স্রেফ aba^{-1}-এর পরপর power বার করে। এই power বার করার সময়ে একটা জিনিসে বেশ সুবিধা হয়েছিল, সেটা হল a^{-1} আর a কেটে যাওয়া। এই ব্যাপারটা যেকোনো power-এর ক্ষেত্রেই হয়, যেমন

$$\left(aba^{-1}\right)^3 = ab\underbrace{a^{-1}a}b\underbrace{a^{-1}a}ba^{-1} = ab^3a^{-1}.$$

সুতরাং যদি $o(b) = 3$ বলা থাকত, তবে $o\left(aba^{-1}\right)$-ও হত 3. অর্থাৎ in general বলতে পারি $o\left(aba^{-1}\right)$ সর্বদাই $o(b)$-এর সমান হবে। এই গুরুত্বপূর্ণ জিনিসটাই দেখাতে বলেছে নীচের অংকটায়।
এই প্রসঙ্গে বলে রাখি যে, b আর aba^{-1}-কে বলে পরস্পরের **conjugate**। এদের নিয়ে পরে আমরা আরো আলোচনা করব।

Example 54: In a finite group $(G, \bullet)$ show that a and xax^{-1} are of the same order for any two elements $a, x \in G$.[2] **(2004)**

SOLUTION:

> Let $b = xax^{-1}$.

> Then, for any $i \in \mathbb{N}$,
>
> $$b^i = \underbrace{(xax^{-1})(xax^{-1})\cdots(xax^{-1})}_{i \text{ times}}$$
> $$= xa(x^{-1}x)a(x^{-1}x)a\cdots ax^{-1} \quad [\text{ associativity}]$$
> $$= xa^ix^{-1}.$$
>
> So for any $i \in \mathbb{N}$,
>
> $$a^i = e \iff \left(xax^{-1}\right)^i = e \iff b^i = e.$$
>
> Hence, if n is the least positive integer for which $a^n = e$, then n is also the least positive integer for which $b^n = e$.
>
> So $o(a) = o(b)$, as required.

■

সমাধানটার দিকে তাকালেই দেখবে যে এখানে G-এর finiteness কোথাও কাজে লাগেনি। G যদি infinite হত, তবে $o(a)$ আর $o(b)$-এর পক্ষে ∞ হওয়া সম্ভব, কিন্তু সেক্ষেত্রেও সব সময়ে $o(a) = o(b)$ হতেই হবে। যদি ∞-ও হয়, তো দুজনে একই সঙ্গে ∞ হবে।

Example 55: In a group G prove that $\left(a^{-1}\right)^{-1} = a$ where $a \in G$. Hence show that every group of even order contains an element of order 2.[5] **(1999)**

SOLUTION: প্রথম অংশটা তো আগেই করেছি, Example 21-এ। দ্বিতীয় অংশটায় হাত দেওয়ার আগে একটা ধাঁধা করা যাক। একটা ঘরে মোট 10 জন ভদ্রলোক ভদ্রমহিলা আছেন। তাঁদের মধ্যে যারা বিবাহিত তাঁরা স্বামীস্ত্রী দুজনেই ঘরের মধ্যে আছেন। রামবাবু বলে একজন ভদ্রলোক ঘরের মধ্যে আছেন, যিনি অবিবাহিত। তোমাকে দেখাতে হবে যে, রামবাবুই ঘরের মধ্যে একমাত্র অবিবাহিত মানুষ হতে পারেন না, অন্ততঃ আরেকজন কেউ অবিবাহিত থাকতে বাধ্য।

কেন? কারণ, বিবাহিতরা সবাই জোড়ায় জোড়ায় আছেন, ফলে মোট বিবাহিত লোকের সংখ্যা জোড় হবেই। ঘরে যেহেতু মোট 10 আছেন, আর 10 একটা জোড় সংখ্যা, তাই অবিবাহিতদের সংখ্যাও জোড় হবে। রামবাবু তাঁদের মধ্যে একজন, তিনিই যদি একমাত্র অবিবাহিত হতেন, তবে তো অবিবাহিতদের সংখ্যা হত 1, মানে বিজোড়!

ঠিক একই যুক্তিতে এই অংকটাও হবে। G-এর element-দের order হবে $1, 2, 3, \ldots$ ইত্যাদি। এর মধ্যে একজনেরই খালি order হবে 1, সে হল identity. আমাদের দেখাতে হবে অন্ততঃ একজনের order হবে 2. তাহলে বাকি যদি কেউ পড়ে থাকে, তাদের order হবে > 2. এদের set-টাকে নিয়ে শুরু করি--

> Let $H = \{a \in G : o(a) > 2\}$.

এরা হল বিবাহিতদের দল। এখানে $o(a) > 2$ মানে হল a আর a^{-1} আলাদা। এদের আমরা একজোড়া স্বামীস্ত্রী হিসেবে ধরছি। আর $a = a^{-1}$ মানে ধরছি, a যেন অবিবাহিত।

> Shall show that $|H|$ is even.
>
> For each element $a \in H$ we have $a^{-1} \in H$, since $o(a^{-1}) = o(a)$.
>
> Also, by the first part, $\left(a^{-1}\right)^{-1} = a$.
>
> So each element a of H can be paired with a distinct element a^{-1} in H,

> So $|H|$ must be even.

H-এর বাইরে যারা আছে (মানে আমাদের উপমায় অবিবাহিতদের দল), তাদের দিকে তাকাই। এদের মধ্যে একজন তো আছেই জানি, identity-টা। তা ছাড়াও কেউ একটা যে আছে সেটাই দেখাতে হবে।

> Since $|G|$ is even, so $|G\backslash H| = |G| - |H|$ must also be even.

এখানে $G\backslash H$ মানে G থেকে H-কে বাদ দিলে যে set-টা পড়ে থাকে।

> Since $e^{-1} = e$, so $e \in G\backslash H$.
> Hence $|G\backslash H| \geq 2$.

এটা কেন হল বুঝলে তো? $|G \setminus H|$ হল even, তার মানে $0, 2, 4, ...$ এইরকম কিছু, 1 হতে পারে না। সুতরাং যেই দেখলাম যে $e \in G \setminus H$ সুতরাং $|G \setminus H| \neq 0$, অতএব $|G \setminus H| \geq 2$. এখানে e-টা রামবাবুর ভূমিকা পালন করছে।

> So $\exists a \in G\backslash H$ such that $a \neq e$. For this a we have $o(a) = 2$, as required.

■

এবার যে কটা অংক করব সেগুলো নিছক কিছু কসরৎ ছাড়া আর কিছুই নয়। যাদের মাথায় পরীক্ষাপাশের দুশ্চিন্তা নেই, তারা আজকের বাকি অংকগুলোর উপর হালকাভাবে চোখ বুলিয়ে ছেড়ে দিতে পারো।

Example 56: If $G = \{1, x, y\}$ is a multiplicative group then show that $x^3 = y^3 = 1$.[3] **(2008)**

SOLUTION: এখানে multiplicative শব্দটা দেখে যেন ঘাবড়ে যেও না। ওটা বস্তুতঃ এখানে অনাবশ্যক। বলতে চেয়েছে যে group-টার binary operation-টাকে আমরা গুণের মত করে লিখব যেমন x, y মিলিয়ে যেটা পাব, তাকে xy লিখব ($x + y$ নয়)। একইভাবে দুটো x মিলিয়ে পাব x^2.
এই অংকটা দুইভাবে করব। প্রথম সমাধানে এই কথাটা ব্যবহার করব যে, group-এর যেকোনো element-এর order দিয়ে group-এর সাইজ ভাগ যায়। এই কথাটা ব্যবহার করলে সমাধানটা সংক্ষেপে হবে। কিন্তু এই জিনিসটা এই বছরের সিলেবাসে নেই। তাই পরের সমাধানে আমরা এটা ব্যবহার করব না, ফলে সমাধানটা একটু লম্বা হবে।

> We know that the order of any element divides the size of the group.
> Here the size of the group is 3.
> So the orders of x and y divide 3.
> Hence $x^3 = y^3 = 1$, as required.

অংকটা অতি অনায়াসে হয়ে গেল বটে, কিন্তু সাবধান! আমরা এ অধ্যায়ে এখনও প্রমাণ করি নি যে, element-এর order দিয়ে group-এর order সব সময়ে ভাগ যায়। সেই প্রমাণটা আসবে পরের অধ্যায়ে (মানে পরের বছরের সিলেবাসে)। অবশ্য এবার যে দ্বিতীয় সমাধানটা করব তাতে সেই সমস্যা নেই--

বিকল্প পদ্ধতি

> Here $x, y, 1$ are all distinct.

কারণ নইলে $G = \{1, x, y\}$ লেখা হত না। যেমন যদি $x = y = 2$ হত তবে তুমি নিশ্চয়ই $\{1, 2\}$ না লিখে খামোখা $\{1, 2, 2\}$ লিখতে না!

We must have $xy \neq x$

⟦ Because:

If $xy = x$, then cancelling x we have
$y = 1 (\Rightarrow\Leftarrow \because y \neq 1)$.

⟧

এখানে $\Rightarrow\Leftarrow$ মানে contradiction বা "অসম্ভব ঘটনা"। আমাদের দেওয়া আছে $y \neq 1$, কিন্তু $xy = x$ হলে হতে হয় $y = 1$. সেটা তো আর হতে পারে না, তাই $xy = x$-ও হতে পারে না।

Similarly, $xy \neq y$.

কিন্তু xy কিছু একটা তো হতে হয়। যদি সেটা x বা y না হতে পারে, তবে পড়ে রইল খালি 1, মানে $xy = 1$ হওয়া ছাড়া পথ নেই।

Since G is closed under multiplication, we must have $xy = 1$.

Now $x^2 \neq x$,

⟦ Because:

If $x^2 = x$, then by cancelling x, we have
$x = 1 (\Rightarrow\Leftarrow \because x \neq 1)$.

⟧

Also, $x^2 \neq 1$,

⟦ Because:

If $x^2 = 1$, then $x^2 = xy$, $(\because xy = 1)$.
So, cancelling x, we have
$x = y (\Rightarrow\Leftarrow \because x \neq y)$.

⟧

So we must have $x^2 = y$.

Hence $x^3 = xx^2 = xy = 1$.

Similarly, $y^3 = 1$, also, as required.

■

Example 57: True or false: Let G be a group and $a, b \in G$, $b \neq e$ (e is the identity element of G). If $o(a) = 3$ and $aba^{-1} = b^2$ then $o(b) = 7$.[2] **(2006)**

SOLUTION:

Given $b \neq e$ and
$$aba^{-1} = b^2. \quad (*)$$
Squaring,
$$aba^{-1}aba^{-1} = b^4,$$
$$\text{or,} \quad abba^{-1} = b^4,$$
$$\text{or,} \quad ab^2a^{-1} = b^4.$$
$\therefore$ By (*),
$$a(aba^{-1})a^{-1} = b^4,$$
or,
$$a^2ba^{-2} = b^4.$$
Since $a^3 = e$, so $a^2 = a^{-1}$.
Hence $a^{-1}ba = b^4$, or $b = ab^4a^{-1}$.
Squaring,
$$b^2 = ab^4a^{-1}ab^4a^{-1} = ab^8a^{-1}. \quad (**)$$
So, from (*) with (**), $ab^8a^{-1} = aba^{-1}$.
Cancelling ab from left and a^{-1} from right, $b^7 = e$.
So $o(b)|7$.
Hence $o(b) = 1$ or 7.
But since $b \neq e$, so $o(b) \neq 1$.
So $o(b) = 7$.
Hence the statement is true.

■

Exercise 31: Let $(G, \circ)$ be a group and $a, b \in G$. If $o(a) = 3$ and $a \circ b \circ a^{-1} = b^2$, find the order of b if b is not the identity element of G.[2] **(2011.17ii)**
HINT:
আগের অংকটাই। ■

Exercise 32: In a finite group $(G, \bullet)$ show that, if for $a \in G$ $a^3 = e$ (identity in G) and $aba^{-1} = b^2$ then order of b is 7.[3] **(2004)**
HINT:
আগের অংকটার মতই দেখতে, কিন্তু এটা আসলে ভুল অংক। কারণ এখানে $b \neq e$. বলতে ভুলে গিয়েছে। সেটা বলা থাকলে ঠিক আগের অংকটাই হত। ■

Example 58: In a group G the element a is of order 2. For some $b \in G$ we have $ab^4a = b^7$.

Show that $b^{33} = e$, where e is the identity element of G.

SOLUTION:

> Since $o(a) = 2$, so $a^2 = e$.

আমাদের আরও দেওয়া আছে--

> Given
> $$ab^4a = b^7. \tag{1}$$

সমস্যা এই যে এতে কিছু কাটাকাটি করার মত নেই, কারণ বাঁদিকের দুইপাশেই a রয়েছে, কিন্তু ডানদিকে কোনো a নেই। কিন্তু যেহেতু $a^2 = e$ দেওয়া আছে, তাই দুটো a-কে পাশাপাশি আনতে পারলে তারা কেটে যাবে। সুতরাং দুটো a-কে পাশাপাশি আনার চেষ্টা করা যাক। কথাটা যত সহজে বললাম, তত সহজে একবারে মাথায় না আসাই স্বাভাবিক। এসবক্ষেত্রে বার কয়েক এদিক ওদিক ঢুঁ মারতেই হয়।

যাই হোক, দুটো a-কে পাশাপাশি আনার একটা পথ হচ্ছে দুই দিককে square করে দেওয়া--

> Squaring,
> $$ab^4aab^4a = b^{14},$$

এইবার মাঝের a দুটো কেটে যাবে--

> and so, since $a^2 = e$,
> $$ab^8a = b^{14}.$$

হঠাৎ দেখে মনে হতে পারে যে, এ তো সেই গোড়ার জিনিসটারই মতন একটা কিছু, এতে আর সুবিধা কি হল? উল্টে b-এর power-গুলো আরো বেড়ে গেল! কিন্তু b-এর power-গুলোকে কমানোর ব্যবস্থা করা কঠিন নয়, কারণ আমরা জানি যে $b^7 = ab^4a$. অর্থাৎ b^7-কে b^4 দিয়ে লেখা যায়। সুতরাং মাঝের ওই b^8-টাকে ভেঙে b^7b হিসেবে লিখব, তারপর b^7-টাকে b^4 দিয়ে লিখব--

> $$\begin{aligned} \therefore b^{14} &= ab^8a \\ &= ab^7ba \\ &= a(ab^4a)ba \quad [\because b^7 = ab^4a.] \\ &= b^4aba \quad [\because a^2 = e.] \end{aligned}$$

তার মানে সব মিলিয়ে দাঁড়াল $b^{14} = b^4aba$. এইবার বাঁদিক থেকে b^4 কাটা যাবে--

> Cancelling b^4 from left,
> $$b^{10} = aba.$$

কিন্তু তাতেই বা কি লাভ হল? সেই তো গোড়ার জিনিসটার মতই আরও একটা জিনিস পেলাম। সত্যিই এভাবে চালালে আমরা একই রকম আরও গুচ্ছ গুচ্ছ equation পাব। সুতরাং equation-এর জঙ্গলে পথ না হারাতে হলে একটু ঠাণ্ডা মাথায় ভাবা যাক। আমরা যা যা পাচ্ছি, তাদের সবারই চেহারা একই রকম--

$$b^{\text{কিছু একটা}} = ab^{\text{কিছু একটা}}a$$

এদিকে আমাদের দেখাতে হবে $b^{33} = e$, যাতে কোনো a নেই। প্রশ্ন হচ্ছে a-টাকে তাড়াব কী ভাবে? যদি কোনো ভাবে আমরা দেখাতে পারি যে, $b^n = ab^ma$ আবার $b^k = ab^ma$ তবে দুটো মিলিয়ে পাব $b^k = b^n$, এবং তা থেকে পাব $b^{k-n} = e$. যদি কোনোভাবে $k - n = 33$ করতে পারি, তবেই কেল্লা ফতে! আমাদের হাতে আছে $b^7 = ab^4a$. যেহেতু $7 + 33 = 40$, সুতরাং b^{40}-এ পৌঁছতে পারলেই হয়! এক্ষুণি আমরা b^{10}-ওয়ালা একটা সমীকরণ পেয়েছি। অতএব--

Raising to the 4th power,

$$b^{40} = abaabaabaaba = ab^4a, \quad (\mathbf{2})$$

since $a^2 = e$.

$(\mathbf{1})$ আর $(\mathbf{2})$-কে তুলনা করলেই বুঝবে যে, সমাধানের আর বড় দেরী নেই--

So, comparing $(\mathbf{1})$ and $(\mathbf{2})$,

$$b^{40} = b^7.$$

Cancelling b^7,

$$b^{33} = e,$$

as required.

■

DAY 18
Subgroup (part 1)

আমরা দেখেছি যে $(\mathbb{R}, +)$ হল একটা group. আবার $(\mathbb{Z}, +)$-ও একটা group. এখানে $\mathbb{Z}$ আবার $\mathbb{R}$-এর একটা subset-ও বটে। এবং দুটো group-এর ক্ষেত্রেই binary operation-টা একই। তাই আমরা $(\mathbb{Z}, +)$-কে বলি $(\mathbb{R}, +)$-এর একটা **subgroup**. এইভাবে একটা group-এর পেটে আরেকটা group ঢুকে বসে থাকার বিস্তর উদাহরণ পাওয়া যায়। কখনও আবার একটার পেটে একটা, তার পেটে আবার আরেকটা, এরকম করে পরপর চলতে থাকে। যেমন $(\mathbb{R}, +)$-এর পেটে আরেকটা subgroup হল $(\mathbb{Q}, +)$, তার মধ্যে আছে $(\mathbb{Z}, +)$.

DEFINITION: Subgroup

Let $(G, \star)$ be a group. Then $H \subseteq G$ is called a **subgroup** if $(H, \star)$ is a again a group.

লক্ষ কর যে, binary operation-টা G এবং H দুজনের ক্ষেত্রেই একই।

Example 59: এমন কোনো group $(G, \star)$ কি সম্ভব, যার কোনো subgroup নেই?

SOLUTION: না, যদি G-র identity হয় e, তবে $H = \{e\}$ অবশ্যই একটা subgroup হবে। একে বলে G-এর **trivial subgroup**. আবার G নিজেই G-এর একটা subgroup. ■

অনেক সময়েই আমরা এই দুটো subgroup বাদে বাকিদের নিয়ে কাজ করতে চাই, তাদের বলা হয় nontrivial, proper subgroup.

Example 60: আমরা এক্ষুণি দেখলাম যে, $(\mathbb{R}, +)$-এর একটা subgroup হল $(\mathbb{Q}, +)$, তার একটা subgroup হল $(\mathbb{Z}, +)$. বলতে পারো $(\mathbb{Z}, +)$-এর পেটের মধ্যে কি কোনো nontrivial, proper subgroup আছে?

SOLUTION: হ্যাঁ, প্রচুর। একটা উদাহরণ হল $2\mathbb{Z}$, মানে যাবতীয় even (জোড়) সংখ্যার set–

$$2\mathbb{Z} = \{2n \;:\; n \in \mathbb{Z}\}.$$

আরেকটা উদাহরণ হল $3\mathbb{Z}$, মানে সেই সব সংখ্যার set যারা 3 দিয়ে ভাগ যায়। দুটোরই প্রমাণ একইরকম। আমরা $2\mathbb{Z}$-এর ক্ষেত্রে প্রমাণটা করে দেখাই। আমরা দেখাতে চলেছি যে, $(2\mathbb{Z}, +)$ একটা group, সুতরাং সেই চারটে শর্ত পরীক্ষা করব।

> Closure: If $a, b \in 2\mathbb{Z}$ then $a = 2m$ and $b = 2n$ for some $m, n \in \mathbb{Z}$. So $a + b = 2(m + n) \in 2\mathbb{Z}$, since $m + n \in \mathbb{Z}$.
>
> Associative: Associativity is inherited from $(\mathbb{Z}, +)$.

এই "inherited" ব্যাপারটা বুঝে নাও। আমাদের দেখানোর দরকার যে, $+$ হল $2\mathbb{Z}$-এর উপর associative. কিন্তু "$2\mathbb{Z}$-এর উপর $+$" আর "$\mathbb{Z}$-এর উপর $+$" তো আর আলাদা কিছু নয়। এদিকে $(\mathbb{Z}, +)$ যে একটা group সে তো আমরা জানিই, সুতরাং $\mathbb{Z}$-এর উপরে $+$ অবশ্যই associative. অতএব $2\mathbb{Z}$-এর উপরেও $+$-টা associative না হয়ে যায় কোথায়? "Inherited" মানে হল "উত্তরাধিকারসূত্রে পাওয়া", এখানে যেন $\mathbb{Z}$-এর সন্তান হল $2\mathbb{Z}$, এবং associativity-টা উত্তরাধিকারসূত্রে পাওয়া গেল।

> Identity: 0 is the identity in $2\mathbb{Z}$, because $0 = 2 \times 0 \in \mathbb{Z}$ and
>
> $$\forall a \in 2\mathbb{Z} \quad 0 + a = a + 0 = a.$$

এইখানে অনেক ছাত্রের গোল বেঁধে যায় দেখেছি-- 0 কি $2\mathbb{Z}$-এর মধ্যে পড়ে, মানে 0 কি একটা even সংখ্যা? অনেককেই বলতে শুনেছি যে, 0-টা নাকি even-ও নয়, odd-ও নয়! সেটা ঠিক কথা নয় মোটেই। Even সংখ্যা তারাই, যাদেরকে $2n$ আকারে লেখা যায়, যেখানে $n \in \mathbb{Z}$. দেখাই যাচ্ছে যে, 0-কে এই আকারে লেখা যায়, কারণ $0 = 2 \times 0$ এবং $0 \in \mathbb{Z}$. সুতরাং 0 অবশ্যই একটা even সংখ্যা। এ নিয়ে সন্দেহমাত্র নেই!

> Inverse: If $a \in 2\mathbb{Z}$ then $-a \in 2\mathbb{Z}$.
>
> ⟦ Because:
>
> $a = 2n$ for some $n \in \mathbb{Z}$. So $-a = 2(-n) \in 2\mathbb{Z}$, as $-n \in \mathbb{Z}$.
>
> ⟧
>
> Also $a + (-a) = (-a) + a = 0$.

■

একইভাবে নীচের অংকটা করো।

Exercise 33: দেখাও যে $3\mathbb{Z}$ হল $(\mathbb{Z}, +)$-এর একটা subgroup. এখানে $3\mathbb{Z}$ মানে সেই সব integer-দের set, যারা 3 দিয়ে ভাগ যায়। ■

এক্ষুণি আমরা "inherited" বলে একটা ব্যাপার শিখলাম। সেইটা কাজে লাগিয়ে নীচের অংকটা কর তো।

Exercise 34: Let G be an Abelian group. Let H be any subgroup of G. True or false: H must be Abelian. ■

এর পরের অংকটা একটু বেশী কঠিন, হয়তো এখনই উত্তরটা মাথায় আসবে না। কিন্তু চিন্তা করতে থাকো, উত্তর দেখে নিও না। নীচের বিভিন্ন উদাহরণের মধ্যে উত্তরের সূত্র লুকিয়ে আছে।

Exercise 35: Let G be a non-Abelian group. Let H be any nontrivial subgroup of G. True or false: H must be non-Abelian.
HINT: এখানে nontrivial বলেছি, কারণ একটা Abelian subgroup তো সব সময়েই আছে, সেই trivial subgroup-টা-- $\{e\}$. প্রশ্ন হল, ওটা বাদে বাকি subgroup-গুলো কি সবাই non-Abelian হবেই? ■

এবার কয়েকটা অংক দিচ্ছি, যেখানে একটা subset-কে পরীক্ষা করে দেখতে হবে সেটা একটা subgroup কিনা। তোমার কাজ হল সংজ্ঞার চারটে শর্ত পরীক্ষা করে দেখা। এতে সমাধানগুলো হয়তো একটু লম্বা হতে পারে। কালকে আমরা একটা নতুন কায়দা শিখব, যা দিয়ে একই অংক একটু সংক্ষেপে করা যাবে।

Exercise 36: আমরা দেখেছি যে, A কোনো set হলে $(\mathscr{P}(A), \Delta)$ সব সময়ে একটা group হয়, যেখানে $\mathscr{P}(A)$ হল A-র power set, আর Δ হল symmetric difference. (যদি ভুলে গিয়ে থাকো, তবে Day 12-এর শেষের দিকটা দেখে নাও।) এবার A-র যে কোনো একটা subset নাও, $B \subseteq A$. দেখাও যে, $\mathscr{P}(B)$ হবে $\mathscr{P}(A)$-র একটা subgroup. ■

Exercise 37: এই অংকটা হল $(\mathscr{P}(A), \Delta)$-র আরেকটা subgroup নিয়ে। যদি $\mathcal{D}$ হয় A-র যাবতীয় <u>finite</u> subset-এর set, তবে দেখাও যে, $\mathcal{D}$ হবে $(\mathscr{P}(A), \Delta)$-র একটা subgroup. ■

Exercise 38: সমবাহু ত্রিভুজ ঘুরিয়ে ফিট করার group-টা মনে আছে? সব মিলিয়ে 6-টা element ছিল সেই group-টায়--

$$\{e, r, \ell, f_1, f_2, f_3\}.$$

পরীক্ষা করে দ্যাখো তো $\{e, f_1\}$ এর একটা subgroup হচ্ছে কিনা। ■

Example 61: হয়তো মনে আছে যে, Example 32-তে আমরা যাবতীয় odd সংখ্যার set থেকে একটা group বানিয়েছিলাম এই binary operation-টা দিয়ে--

$$a \star b = a + b - 1.$$

আমরা কি এই group-টাকে $(\mathbb{Z}, +)$-এর subgroup বলতে পারি?
SOLUTION: না, কারণ যাবতীয় odd সংখ্যার set-টা $\mathbb{Z}$-এর subset হলেও, $\star$ আর $+$ আলাদা binary operation. ■

Binary operation-টা সব সময়ে একটা group এবং তার subgroup-এর ক্ষেত্রে একই হতে হবে। এর ফলে group-এর বিভিন্ন জিনিস subgroup-টা "উত্তরাধিকারসূত্রে" পেতে পারে, যেমন associativity বা commutativity. নীচের theorem-টায় আরেকটা এরকম জিনিসের কথা বলা হয়েছে--identity.

THEOREM

If H is a subgroup of G then the identity of H must be the same as the identity of G.

Proof:

> Let e_1, e_2 be, respectively, the identities of G, H.

দেখাব যে $e_1 = e_2$.

> Then $e_2 e_1 = e_2$ and also $e_2 e_2 = e_2$.

কারণ G-এর যে কোনো element-কেই e_1 দিয়ে গুণ করলে অপরিবর্তিত থাকে। তাই $e_2 \in G$-কে e_1 দিয়ে গুণ করে প্রথম equation-টা পেয়েছি। আবার H-এর যেকোনো element-কে e_2 দিয়ে গুণ করলে অপরিবর্তিত থাকে। যেহেতু $e_2 \in H$, তা থেকে দ্বিতীয় equation-টা এসেছে।

> So $e_2 e_2 = e_2 e_1$.
> So, cancelling e_2 from left, $e_2 = e_1$, as required.

[Q.E.D]

Exercise 39: এই theorem-টাকে একজন ছাত্র এইভাবে প্রমাণ করেছে--

> আমরা জানি $\forall g \in G \quad ge_1 = e_1 g = g$. এদিকে $H \subseteq G$. সুতরাং $\forall h \in H \quad he_1 = e_1 h = h$. অতএব e_1-ও H-এর একটা identity. কিন্তু H তো একটা group, তার তো আর দুটো আলাদা identity থাকতে পারে না। সুতরাং অবশ্যই $e_2 = e_1$.

এই প্রমাণটা কিন্তু ভুল। কেন বল তো! ■

Example 62: Let G be a group and H be a nonempty subset of G. Prove that if H is a subgroup of G, then $HH = H$.[2] **(2014.16a)**

SOLUTION: এখানে HH মানে হল সেই G-র সেইসব সদস্যদের set, যাদেরকে H-এর দুজন element মিলিয়ে লেখা যায়, অর্থাৎ--

$$HH = \{h_1 h_2 \ : \ h_1, h_2 \in H\}.$$

আমাদেরকে বলেছে HH আর H, এই দুটো set-কে সমান দেখাতে। সুতরাং আমরা সেই চিরাচরিত দুইধাপে এগোব--একবার দেখাব $HH \subseteq H$, তারপর দেখাব $H \subseteq HH$.

> If $x \in HH$, then $x = h_1 h_2$ for some $h_1, h_2 \in H$.
> $\because H$ is closed under binary operation, $\therefore x = h_1 h_2 \in H$.
> Hence $HH \subseteq H$.

এবার উল্টো দিকটা--

> Let $y \in H$.
> $\because H$ is a subgroup, $\therefore e \in H$, where e is identity element of G.
> So $y = ey \in HH$, since $e \in H$ and $y \in H$.
> Thus $H \subseteq HH$.
> Combining, $HH = H$, as required.

■

18.1 Intersection

দুটো subgroup-এর intersection সব সময়ে একটা subgroup হয়। কিন্তু ওদের union একটা subgroup নাও হতে পারে। এবার সেই প্রসঙ্গে আলোচনা করব।

Example 63: True or false: The intersection of two subgroups of a group is a subgroup.[2.5] **(1999)**

SOLUTION: হ্যাঁ, দুটো subgroup-এর intersection সর্বদাই একটা subgroup হয়।

> Yes, the statement is true.

কেন true, সেটা বোঝা কঠিন নয়। কখন একটা group-এর subset একটা subgroup হয়? যখন তার মধ্যে বিশেষ কিছু জিনিস থাকে, যেমন identity থাকে, প্রতিটি element-এর inverse থাকে, এইরকম। যেহেতু আমরা দুটো subgroup নিয়েই শুরু করছি, তার মানে এইসব জিনিস তাদের দুজনের মধ্যেই আছে, আর দুজনের মধ্যে যুগপৎ থাকা মানেই তো তাদের intersection-এর মধ্যে থাকা!

এইবার এই কথাটাকে অংকের ভাষায় লিখতে হবে। আজকে আমরা এই প্রমাণটা সরাসরি সংজ্ঞা থেকে করব (চারটে শর্ত পরীক্ষা করে)। কালকে একটা নতুন কায়দা শিখব, যেটা দিয়ে এই একই অংক অনেকটা সংক্ষেপে করা যাবে।

এখানে অংকটাতে কোনো group বা subgroup-এর নাম দেওয়া নেই। কিন্তু এদের নাম না দিলে লেখা মুস্কিল, তাই আমরাই বিভিন্ন জিনিসপত্রের নাম দিয়ে নিই গোড়াতে--

> Let $(G, *)$ be a group. Let H_1, H_2 be two subgroups of G.
>
> To show that $H = H_1 \cap H_2$ is a subgroup of G.

এটা আমরা সরাসরি সংজ্ঞা থেকে দেখাব।

> <u>Closure:</u> Shall show
>
> $\forall a, b \in H \quad a * b \in H.$

এক্ষুণি যে যুক্তিটার কথা বললাম সেটাই লাগাব--$a * b$ আছে H_1 এবং H_2 দুজনেরই মধ্যে, অতএব $H_1 \cap H_2$-এর মধ্যেও থাকতে বাধ্য।

$\forall a, b$

> Take any $a, b \in H$.
>
> $\because a, b \in H_1, \therefore a * b \in H_1.$
> Similarly, $\because a, b \in H_2, \therefore a * b \in H_2.$
> So $a * b \in H_1 \cap H_2 = H$, as required.

এরপরের কাজ associative দেখানো। যথারীতি "উত্তরাধিকার"-এর গল্প--

> <u>Associativity:</u> inherited from G.

আর বাকী থাকে identity এবং inverse দেখানো। সে দুটোই আমাদের আগের যুক্তি অনুযায়ী হবে--

> Identity:
>
> $\because H_1, H_2$ are subgroups,
>
> $\therefore e \in H_1$ and $e \in H_2$.
>
> $\therefore e \in H_1 \cap H_2 = H$.
>
> Inverse:
>
> Take any $a \in H$.
>
> $\because H_1, H_2$ are subgroups, $\therefore a^{-1} \in H_1$ and $a^{-1} \in H_2$.
>
> $\therefore a^{-1} \in H_1 \cap H_2 = H$.
>
> Thus, H is a subgroup, as required.

■

দুটো subgroup-এর intersection-কে এভাবে subgroup দেখালাম, ঠিক একইভাবে যতগুলো খুশী subgroup-এর intersection-কেও subgroup দেখানো যাবে। এমন কি infinite-সংখ্যক subgroup-এর intersection হলেও! সুতরাং পেলাম--

> **THEOREM**
>
> Arbitrary intersection of subgroups is again a subgroup.

তোমরা যারা real analysis পড়েছ, তারা লক্ষ করবে যে, subgroup-এর সঙ্গে এই ব্যাপারে closed set-এর মিল আছে। সেখানেও ছিল যে, arbitrary intersection of closed sets is again closed.

18.2 Union

এতক্ষণ intersection নিয়ে আলোচনা করলাম, এবার union নিয়ে করি।

Example 64: True or false: If H, K are two subgroups of a group $(G, \bullet)$, then $H \cup K$ is also a subgroup of $(G, \bullet)$.[2] **(2000)**

SOLUTION:

> The statement is not true in general.

কী করে বুঝলাম এই কথাটা? কারণ প্রথম কথা এই যে, $H \cup K$-কে যদি subgroup হতে হয়, তবে তাকে closed under $\bullet$ হতে হবে। কিন্তু যদি $a, b \in H \cup K$ এমনভাবে নিই যাতে $a \notin H$ আর $b \notin K$ হয়, তবে $a \bullet b$-টা H-এও পড়বে না, K-তেও পড়বে না। এই চিন্তার ভিত্তিতে এবার একটা counterexample বানাতে হবে।

> Let $G = (\mathbb{Z}, +)$.
>
> Take $H = 2\mathbb{Z}$ and $K = 3\mathbb{Z}$. Then H and K are subgroups of G. But $H \cup K$

is not a subgroup,

because $2, 3 \in H \cup K$ but $2 + 3 = 5 \notin H \cup K$.

কারণ 5 সংখ্যাটা 2 বা 3 কোনোটা দিয়েই ভাগ যায় না। ■

দুটো subgroup-এর union যে subgroup নাও হতে পারে, সেটা আমরা দেখলাম। কিন্তু দুটো subgroup-এর union কি কখনোই একটা subgroup হতে পারে না? হ্যাঁ পারে, একটা বিশেষ ক্ষেত্রেই খালি পারে--যদি একটা subgroup অন্যটার পেটের ভিতরে থাকে। কারণ সেক্ষেত্রে union-টা হবে বড় subgroup-টাই।

Example 65: Let $(G, *)$ be a group and S_1, S_2 be two subgroups of $(G, *)$. Then $S_1 \cup S_2$ forms a subgroup of $(G, *)$ if and only if either $S_1 \subseteq S_2$ or $S_2 \subseteq S_1$.[5] **(2005,2008)**

SOLUTION: প্রথমে লিখে নিই কী দেওয়া আছে আর কী দেখাতে হবে--

Given: $(G, *)$ group. S_1, S_2 subgroups.

To show:

$$S_1 \cup S_2 \text{ is subgroup} \iff (S_1 \subseteq S_2 \text{ or } S_2 \subseteq S_1).$$

এরকম যেকোনো প্রমাণে সাধারণতঃ $\iff$ -টাকে দুই ভাগে ভেঙে একবার $\implies$ আর তারপরে $\impliedby$ অংশটা দেখাতে হয়। যেই অংশটা খুশী আগে করা যায়।

$(\impliedby)$:

If $S_1 \subseteq S_2$, then $S_1 \cup S_2 = S_2$, which is a subgroup, as required.

If $S_2 \subseteq S_1$, then $S_1 \cup S_2 = S_1$, which is a subgroup, as required.

পরের অংশটা contradiction দিয়ে প্রমাণ করব। এরকম প্রমাণ শুরু হয় যা দেখাতে হবে, তার উল্টোটা ধরে নিয়ে। দেখাতে হবে যে, হয় $S_1 \subseteq S_2$ বা $S_2 \subseteq S_1$. সুতরাং আমরা ধরে নেব যে, এ দুটোর কোনোটাই নয়--

$(\implies)$:

Given: $S_1 \cup S_2$ is a subgroup.

Let, if possible, $S_1 \not\subseteq S_2$ and $S_2 \not\subseteq S_1$.

Pick $a \in S_1 \setminus S_2$ and $b \in S_2 \setminus S_1$. Since $a, b \in S_1 \cup S_2$, so $a * b \in S_1 \cup S_2$, since $S_1 \cup S_2$ is a subgroup.

এমনটা হবার কারণ হল-- দেওয়া আছে $S_1 \cup S_2$ একটা subgroup, তাই $S_1 \cup S_2$ নিশ্চয়ই closed under $*$.

Thus, either $a * b \in S_1$ or $a * b \in S_2$.

দুটো কেসে ভেঙে নিই। প্রথম কেস হল $a * b \in S_1$--

Case I: If $a * b \in S_1$ then

$$b = a^{-1} * (a * b) \in S_1 \quad (\because a \in S_1 \implies a^{-1} \in S_1),$$

> which is impossible, since $b \in S_2 \setminus S_1 (\Rightarrow\Leftarrow)$.

এবার দ্বিতীয় কেস, $a * b \in S_2$--

> Case 2: If $a * b \in S_2$ then
>
> $$a = (a * b) * b^{-1} \in S_2 \quad (\because b \in S_2 \implies b^{-1} \in S_2),$$
>
> which is impossible, since $a \in S_1 \setminus S_2 (\Rightarrow\Leftarrow)$.

■

Exercise 40: Prove that the union of two subgroups H, K of a group $(G, \star)$ forms a subgroup if and only if either $H \subset K$ or $K \subset H$.[3] **(2011.18i)**
HINT:
আগের অংকটাই। এখানে "$\subset$" চিহ্নটা নিয়ে কিছু কথা বলা দরকার। "$\leq$" মানে যেমন "less than or equal to" এবং "$<$" মানে "strictly less than". এই নিয়ে কোনো মতভেদ নেই। কিন্তু $\subseteq$ এবং $\subset$ চিহ্নদুটো নিয়ে সামান্য মতভেদ আছে--

- অনেকে $\subseteq$ দিয়ে বোঝায় "subset or equal to" আর "$\subset$" দিয়ে বোঝায় "strict subset of".
- আবার কেউ কেউ $\subset$ চিহ্ন দিয়ে বোঝায় "subset or equal to." তারা যদি strict subset বোঝাতে চায়, তবে $\subsetneq$ লেখে।

এখানে এই দ্বিতীয় অর্থে ব্যবহার করা হয়েছে। কারণ $H \cup K$-কে subgroup হওয়ার জন্য $H \subseteq K$ বা $K \subseteq H$ হওয়াই যথেষ্ট, কোনো strict subset-এর প্রয়োজন নেই। ■

Example 66: True or false: Let H_1, H_2 be two subgroups of a group G. If $H_1 \cup H_2$ is a subgroup of G and $H_1 \not\subseteq H_2$ then $H_2 \subseteq H_1$.[2.5] **(1998)**
SOLUTION: এই অংকটা আসলে আগের অংকটাকেই অন্যভাবে দেওয়া।

> The result is false. Let, if possible, $H_2 \not\subseteq H_1$.
> Then pick $a \in H_1 \backslash H_2$ and $b \in H_2 \backslash H_1$.

এবার সেই আগের অংকের পথেই এগোব।

> $\because a, b \in H_1 \cup H_2,$ and $\because H_1 \cup H_2$ is a group,
> $\therefore ab \in H_1 \cup H_2.$

দুটো কেস--

> Case 1: $ab \in H_1 :$ $\because a \in H_1, \therefore a^{-1} \in H_1$
> $\therefore a^{-1}ab = b \in H_1 (\Rightarrow\Leftarrow \because b \notin H_1).$

দ্বিতীয় কেস--

Case 2: $ab \in H_2$:
$\because b \in H_2, \therefore b^{-1} \in H_2$
$\therefore abb^{-1} = a \in H_2 (\Rightarrow\Leftarrow \because a \notin H_2)$.

■

DAY 19
Subgroup (part 2)

19.1 সহজে subgroup দেখানো

একটা group $(G, \star)$ আর তার একটা subset $H \subseteq G$ দিয়ে যদি পরীক্ষা করতে বলি H-টা একটা subgroup কিনা, তবে একটা কায়দা হল সরাসরি সংজ্ঞা ব্যবহার করে পরীক্ষা করা যে $(H, \star)$ একটা group হচ্ছে কিনা। এর জন্য চারটে জিনিস দেখাতে হয়--closure, associativity, identity আর inverse. এদের মধ্যে associativity অবশ্য পাওয়া যায় G থেকে উত্তরাধিকারসূত্রেই। এবার দেখব যে, বাকি তিনটেকেও আলাদা করে না দেখালেও চলে, ওদেরকে মিলিয়ে খালি দুটো শর্ত বানানো যায়--

1. $H \neq \phi$,
2. যদি $a, b \in H$ হয়, তবে $a \star b^{-1} \in H$ হবে।

এই দুটো শর্ত দেখাতে পারলেই H-কে subgroup দেখানো হয়ে যায়। বুঝতেই পারছ এই দুটো শর্ত কেন সংজ্ঞার তিনটে শর্তের চেয়ে দেখানো সাধারণতঃ বেশী সহজ--

- $e \in H$ দেখানোর চেয়ে H-এর মধ্যে অন্ততঃ একটা element আছে দেখানো সোজা,
- closure এবং inverse-কে আলাদা করে দেখানোর বদলে

$$a \star b^{-1} \in H$$

দেখিয়ে এক ঢিলে দুই পাখি মেরে দিচ্ছি।

কিন্তু এই শর্টকাটটা যে কাজ করবেই, সেটা কী করে জানলাম? প্রমাণটা চেয়েছে নীচের অংকে।

Example 67: Let $(G, *)$ be a group. A nonempty subset S of G forms a subgroup of $(G, *)$ iff

$$a \in S, b \in S \implies a * b^{-1} \in S.$$

[5] **(2000,2005,2007,2014)**

SOLUTION:

Only if part: Given: S is a subgroup of G, and $a, b \in S$.
Shall show that $a * b^{-1} \in S$.
Since S is a subgroup, so $b^{-1} \in S$. Since S is closed under $*$ we have $a * b^{-1} \in S$, as required.
If part:

Given:

$$\forall a, b \in S a^{-1} * b \in S. \qquad (*)$$

To show: S is a subgroup of G.

S তো দেওয়াই আছে G-এর একটা subset. সুতরাং এটা দেখালেই চলবে যে $(S, *)$ একটা group. আমাদের যথারীতি চারটে জিনিস দেখাতে হবে--closure, associativity, identity আর inverse. অধিকাংশ অংকের ক্ষেত্রেই আমরা প্রথমে closure, তারপর associativity এইভাবে এগোই। কিন্তু এক্ষেত্রে প্রথমে associativity, তারপর identity, তারপর inverse এবং সব শেষে closure দেখালে সুবিধা হবে।

Associativity: inherited from G.

Identity: Shall show $e \in S$, where e is the identity of G.

$\because S \neq \phi$, we can take any $c \in S$.

Taking $a = b = c$ in (*) we have

$$c * c^{-1} \in S.$$

But $c * c^{-1} = e$. So $e \in S$.

Inverse: To show

$$\forall c \in S \quad c^{-1} \in S.$$

Take any $c \in S$.

Taking $a = e (\in S$, as shown) and $b = c$ in (*) we have

$$e * c^{-1} \in S,$$

and so $c^{-1} \in S$.

Closure: To show

$$\forall c, d \in S \quad c * d \in S.$$

Take any $c, d \in S$.

Taking $a = c$ and $b = d^{-1} (\in S$, as shwon) in (*) we have

$$a * b^{-1} = c * \left(d^{-1}\right)^{-1} = c * d \in S,$$

as required.

■

Exercise 41: Let G be a group, and H be a nonempty subset of G. Show that H will be a subgroup of the group G if and only if $a^{-1}b \in H$ for all $a, b \in H$.[5] **(2003)**

HINT:

ঠিক আগের অংকটার মতোই, খালি আগের অংকটায় ছিল ab^{-1}, আর এখানে তার জায়গায় $a^{-1}b$. কিন্তু প্রমাণের কায়দাটা একই থাকবে। ■

আমরা closure এবং inverse শর্তদুটোকে মিলিয়ে একটা শর্ত বানিয়েছিলাম--

$$\forall a, b \in H \quad ab^{-1} \in H.$$

যদি H-টা finite হয়, তবে ব্যাপারটা আরও সহজ হয়ে যায়--inverse শর্তটাকে নিয়ে আদৌ মাথা ঘামাতেই হয় না, খালি closure দিয়েই কাজ হয়ে যায়! সেটাই নীচের অংকটার বক্তব্য।

Example 68: Let $(G, \bullet)$ be a group and H be a nonempty finite subset of G. Prove that $(H, \bullet)$ is a subgroup of $(G, \bullet)$ if and only if

$$a \in H, \quad b \in H \implies a \bullet b \in H.$$

[5] **(2012.18)**

SOLUTION:

> Closure: We are already given that
>
> $$\forall a, b \in H \quad a \bullet b \in H.$$
>
> Associativity: Inherited from G.

এইবার আমরা দেখাব $e \in H$, এবং সেই কাজে H-এর finiteness ব্যবহার করব। আমরা জানি যে, S যদি যে কোনো finite set হয় আর $f : S \to S$ হয় যে কোনো one-one function, তবে f অবশ্যই onto হতেও বাধ্য। এইটা আমরা শিখেছিলাম এই বইয়ের প্রথম অধ্যায়ে, যেখানে "Finite set-এর মজা" আলোচনা করেছিলাম। এই কথাটাই এখানে কাজে লাগবে।

> Identity: Since $H \neq \phi$, we can pick some $a \in H$.
>
> Consider the function $f : H \to H$ defined as $f(h) = a \bullet h$.
>
> This function is well-defined since H is closed under $\bullet$.
>
> Clearly f is one-one.
>
> ⟦ Because:
>
> $f(h) = f(h') \implies a \bullet h = a \bullet h' \implies h = h'$ by left cancellation of a.
>
> ⟧
>
> Since H is finite, hence f is also onto.
>
> So $\exists h \in H \quad f(h) = a$,
>
> or $a \bullet h = a$, or $h = e$, by left cancellation of a.
>
> Hence $e \in H$.

এবার inverse দেখানোর পালা। এখানেও একইভাবে H-এর finiteness কাজে আসবে।

> Inverse: Shall show $\forall a \in H \quad a^{-1} \in H$.
> Take any $a \in H$.
> Consider the function $f(h) = a \bullet h$ again. As above, it is onto.
> So $\exists h \in H \quad f(h) = e$,
> ie, $a \bullet h = e$, or $h = a^{-1}$.
> Hence $a^{-1} \in H$, as required.

■

এই প্রমাণে আমরা H-এর finiteness দুই জায়গায় কাজে লাগিয়েছি। সেটা কি সত্যিই দরকার ছিল? নীচের অংকটা সেই বিষয়ে আলোকপাত করতে সাহায্য করবে।

Exercise 42: আমরা জানি $(\mathbb{Z}, +)$ একটা group, এবং $\mathbb{N} \subseteq \mathbb{Z}$ হল একটা infinite subset. বল তো $\mathbb{N}$ কি closed under $+$? এবার বল তো $(\mathbb{N}, +)$ কি একটা group? এ থেকে কী মনে হয়--আগের অংকে H-এর finite হওয়াটা কি সত্যিই দরকার ছিল? ■

19.1.1 কিছু প্রয়োগ

একটা group-এর কোনো subset দেওয়া থাকলে সেটা subgroup হয় কিনা পরীক্ষা করার একটা সহজ কায়দা শিখলাম। এবার তার কিছু প্রয়োগ দেখি। প্রথমে শুরু করি একটা অংক দিয়ে যেটা আগেই করেছি। তখন করেছিলাম সরাসরি সংজ্ঞা দিয়ে। এবার সহজ কায়দাটা দিয়ে করে দ্যাখো পরিশ্রম কতটা বাঁচে।

Example 69: True or false: The intersection of two subgroups of a group is a subgroup.[2.5] **(1999)**

SOLUTION:

> Let H_1, H_2 be subgroups of a group G.
> Then $e \in H_1$ and $e \in H_2$, where e is the identity of G.
> $\therefore e \in H_1 \cap H_2$.
> Thus $H_1 \cap H_2 \neq \phi$.

ব্যস্ প্রথম শর্ত দেখানো হয়ে গেল। এবার দ্বিতীয় শর্ত--

> Let $a, b \in H_1 \cap H_2$.
> Then $b^{-1} \in H_1$ and $b^{-1} \in H_2$.
> So $ab^{-1} \in H_1$ and $ab^{-1} \in H_2$.
> Thus $ab^{-1} \in H_1 \cap H_2$.
> Hence, by standard result, $H_1 \cap H_2$ is a subgroup of G, as required.

■

Example 70: Let G be a group and g be some fixed element of G, and H be a subgroup of G. Prove that the subset

$$K = \{ghg^{-1} : h \in H\}$$

is a subgroup of G.[2] **(2008)**

SOLUTION:

Clearly, $K \neq \phi$, since $H \neq \phi$.

By standard result, enough to show

$\forall a, b \in K \quad ab^{-1} \in K$.

$\forall a, b$

Take any $a, b \in K$.

Then $a = gh_1g^{-1}$ and $b = gh_2g^{-1}$ for some $h_1, h_2 \in H$.

So, using associativity,

$$\begin{aligned} ab^{-1} &= (gh_1g^{-1})(gh_2g^{-1})^{-1} \\ &= (gh_1g^{-1})\left((g^{-1})^{-1}h_2^{-1}g^{-1}\right) \\ &= (gh_1g^{-1})(gh_2^{-1}g^{-1}) \\ &= gh_1h_2^{-1}g^{-1}. \end{aligned}$$

Now $h_1h_2^{-1} \in H$, because H is a subgroup.

$\therefore ab^{-1} = gh_1h_2^{-1}g^{-1} \in K$, as required.

■

Example 71: Let H be a subgroup of a group G. Show that for any $g \in G$

$$K = gHg^{-1} = \{ghg^{-1} \ : \ h \in H\}$$

is a subgroup of G and $|K| = |H|$.[3] **(2010.3cii)**

SOLUTION: প্রথম অংশটা তো আগের অংকেই করেছি। এবার দ্বিতীয় অংশটা। দুটো set-এর সাইজ সমান দেখাতে বলেছে। তার জন্য একটা ভালো কায়দা হল এটা দেখানো যে, ওদের মধ্যে একটা bijection আছে।

Consider the function $f : H \to K$ defined as

$$f(h) = ghg^{-1}.$$

This function is well-defined since for each $h \in H$ the element ghg^{-1} is in K.

By definition of K, we see that f is onto.

Also f is one-one.

⟦ Because:

If for $h_1, h_2 \in H$ we have $f(h_1) = f(h_2)$, then
$gh_1g^{-1} = gh_2g^{-1}$.
So, cancelling g, g^{-1} from left and right, respectively,
we have $h_1 = h_2$.

⟧

Thus, $f : H \to K$ is a bijection.

So $|H| = |K|$, as required.

■

Exercise 43: Let $(H, *)$ be a subgroup of a group $(G, *)$ and let $a \in G$. Define

$$aHa^{-1} = \left\{aha^{-1} \mid h \in H\right\}.$$

Show that $(aHa^{-1}, *)$ is a subgroup of the group G. Also prove that $|H| = |aHa^{-1}|$.[5] **(2013.18)**
HINT: আগের অংকটারই মত। ■

Example 72: In a group G, $(ab)^3 = a^3b^3$ for all $a, b \in G$. Show that

$$H = \{x^3 : x \in G\}$$

is a subgroup of G.[2] **(2006)**
SOLUTION: আমরা দেখাব যে, $H \neq \phi$ এবং

$$\forall a, b \in H \quad a^{-1}b \in H.$$

<u>Step 1:</u>

Since $G \neq \phi$ so $H \neq \phi$.

<u>Step 2:</u> Shall show

$\forall a, b \in H \quad ab^{-1} \in H.$

$\forall a, b$ Take any $a, b \in H$.

লক্ষ কর যে এখানে H তৈরী হয়েছে যাবতীয় cube-দের নিয়ে। মানে H-এর যেকোনো element-ই কারো না কারো cube.

Then $a = x^3$ and $b = y^3$ for some $x, y \in G$.

So

$$\begin{aligned} ab^{-1} &= x^3(y^3)^{-1} \\ &= x^3(y^{-1})^3 \\ &= (xy^{-1})^3 \quad \left[\text{by given condition}\right] \\ &\in H. \end{aligned}$$

So, by standard result, H is a subgroup of G, as required.

■

Example 73: Let G be an Abelian group. Prove that the subset

$$H = \{g \in G \ : \ g^2 = e(\text{identity element})\}$$

forms a subgroup of G.[2] **(2014.18b)**

SOLUTION:

Since $e^2 = e$, hence $e \in H$. So $H \neq \phi$.
Also, if $a, b \in H$, then

$$\begin{aligned} (ab^{-1})^2 &= ab^{-1}ab^{-1} \\ &= a^2\left(b^{-1}\right)^2 \quad [\because G \text{ is Abelian}] \\ &= a^2\left(b^2\right)^{-1} \\ &= ee^{-1} \quad [\because a, b \in H] \\ &= e. \end{aligned}$$

So $ab^{-1} \in H$.
Hence, by standard, result, H is a subgroup of G.

■

19.2 Centre of a group

একটা group-এর নানা রকম subgroup থাকতে পারে। এদের মধ্যে কিছু কিছু subgroup-এর বিশেষ গুরুত্ব আছে। এরকম একটা subgroup-এর সঙ্গে পরিচয় করা যাক, যার নাম হল **centre.**

Example 74: Define the centre $Z(G)$ of a group G and show that it is a subgroup of G.[1+2] **(2009.3cii)**

SOLUTION:

DEFINITION: Centre of a group

Let G be a group. Then its centre is defined as the subset

$$Z(G) = \{a \in G \mid \forall x \in G \quad xa = ax\}.$$

ব্যাপারটাকে এইভাবে ভাবতে পারো--centre-টা তৈরী হয়েছে খালি মিশুকে element-দের নিয়ে। মিশুকে তো, তাই এরা সবার সঙ্গেই commute করে।
$Z(G)$-কে subgroup দেখানোর জন্য আবার সেই দুই ধাপের কায়দা লাগাব--

Step 1: Shall show that $Z(G) \neq \phi$:

Let e be the identity of G. Then we know that

$$\forall x \in G \quad ex = xe.$$

So $e \in Z(G)$. Hence $Z(G) \neq \phi$.

Step 2: Shall show

$\forall a, b \in Z(G) \quad ab^{-1} \in Z(G)$.

$\forall a, b$ Take any $a, b \in Z(G)$.

To show $ab^{-1} \in Z(G)$, ie,

$\forall x \in G \quad ab^{-1}x = xb^{-1}$.

$\forall x$ Take any $x \in G$.

Then

$$\begin{aligned} xab^{-1} &= axb^{-1} \quad [\because a \in Z(G)] \\ &= a(x^{-1})^{-1}b^{-1} \\ &= a(bx^{-1})^{-1} \\ &= a(x^{-1}b)^{-1} \quad [\because b \in Z(G)] \\ &= ab^{-1}(x^{-1})^{-1} \\ &= ab^{-1}x, \end{aligned}$$

as required.

So, by standard, result, $Z(G)$ is a subgroup of G.

■

Exercise 44: Let G be a group. Let $Z(G)$ be a subset of G defined as follows:

$$Z(G) = \{a \in G \mid xa = ax \quad \forall x \in G\}.$$

Prove that $Z(G)$ is a subgroup of G.[2] **(2011.18ii)**
HINT:
উত্তর তো রয়েছে আগের অংকেই। ■

DAY 20
Group-এর পূর্বপুরুষরা

আমরা এই অধ্যায়ের গোড়াতে একটা binary operation-এর বিভিন্ন ভালো ভালো গুণের একটা তালিকা দিয়েছিলাম-- associativity, commutativity ইত্যাদি। এগুলো সব যদি একসঙ্গে চাপাই তবে পাওয়া যায় Abelian group. যদি commutativity বাদ দিই, তবে হয় এমনি group. যদি আরও কম শর্ত চাপাই তবে অন্য কিছু জিনিস পাওয়া যায়, যাদের ভূমিকা অংকের জগতে অপেক্ষাকৃত কম। এবার এদের সংক্ষিপ্ত পরিচয় নেওয়া যাক।
যদি যে কোনো একটা nonempty set এবং তার উপর যে কোনো একটা binary operation নিই, তবে তাকে বলে groupoid. এর কথা এই অধ্যায়ের গোড়ার দিকে একবার এসেছিল। সংজ্ঞাটা এই রকম--

DEFINITION: Groupoid

A **groupoid** $(S, \star)$ means a nonempty set S together with a binary operation $\star$ defined on it.

মনে রেখো যে, binary operation কথাটার মধ্যে closure property-টা ধরা আছে।
যদি এর উপর আমরা associativity চাপাই, তবে পাই একটা semigroup–

DEFINITION: Semigroup

A **semigroup** $(S, \star)$ means a nonempty set S together with an associative binary operation $\star$ defined on it.

যদি এর সঙ্গে আবার identity-ও থাকে তবে সেটা আরও কাজের জিনিস, তাকে বলে একটা monoid (মনয়েড), যেটা computer science-এ বেশ কাজে লাগে।

DEFINITION: Monoid

A **monoid** $(S, \star)$ means a nonempty set S together with an associative binary operation $\star$ defined on it, such that $\star$ has an identity $e \in S$, *i.e.*,

$$\forall s \in S \quad e \star s = s \star e = s.$$

এর উপর যদি আরও শর্ত চাপাই যে, প্রতিটা element-এর inverse-ও থাকতে হবে, তবেই পৌঁছে যাব group-এ, যার উদাহরণ এই অধ্যায়ে অনেক দেখেছি। এবার বাকিদের একটা করে উদাহরণ দেখা যাক।

Example 75: Groupoid-এর উদাহরণ বানানো সবচেয়ে সোজা--যা খুশী একটা nonempty set নাও, ধরো $S = \{1, 2, 3\}$. এবার এর উপরে যা খুশী একটা binary operation $\star$ নাও, যেমন ধরো

$$\forall i, j \in S \quad i \star j = 1.$$

ব্যস্, $(S, \star)$ হয়ে গেল একটা groupoid! ■

Example 76: যদি পরিচিত কোনো set আর binary operation দিয়ে groupoid বানাতে চাও, তাহলে $(\mathbb{Z}, -)$ নিতে পারো। চাইলে $(\mathbb{Z}, +)$-ও নিতে পারো। Groupoid মানে এমন তো কেউ বলে নি যে associativity, commutativity ইত্যাদি থাকলে চলবে না! ■

এবার একটা semigroup বানানো যাক। যে কোনো group-ই একটা semigroup-ও বটে। কিন্তু এবার এমন একটা উদাহরণ দেব যেটা semigroup, কিন্তু group নয়, এমন কি monoid-ও নয়।

Example 77: যদি পরপর কিছু 0 আর 1 লিখে যাই (finite-সংখ্যক), যেমন--

"00111", "0101", "00", "1", "0", "000", ইত্যাদি,

তবে তাদের বলে একেকটা binary string. একটা binary string-এ কতগুলো 0 বা 1 আছে তাকে বলব তার দৈর্ঘ্য, যেমন "0010"-র দৈর্ঘ্য হল 4. ধরো S হল সেই সব binary string-এর set, যাদের দৈর্ঘ্য ≥ 2. এর উপর একটা binary operation $\bullet$ দেব এইরকম--যদি $a, b \in S$ হয় তবে $a \bullet b$ মানে হল a-র পর b-কে জুড়ে দেওয়া। যেমন, $a =$"001" আর $b =$"0111" হলে

$a \bullet b =$"0010111".

একটু চিন্তা করলেই দেখবে যে, এটা একটা associative binary operation. এখানে আমরা length ≥ 2 নিয়েছিলাম, কিন্তু ≥ 3 বা ≥ 4 ইত্যাদি নিলেও চলত। চাইলে তুমি length ≥ 1-ও নিতে পারতে। ■

লক্ষ কর যে, এই semigroup-টা একটা monoid নয়, কারণ এখানে কোনো identity নেই। তুমি একটা binary string-এর পরে আরেকটা binary string জুড়ে দিলে পুরোটা মিলে একটা নতুন binary string হয়ে যেতে বাধ্য। কিন্তু একটু কায়দা করলেই এটাকে আমরা একটা monoid-এ পরিণত করতে পারি। যদি S-এর মধ্যে 0 length-এর binary string-ও রাখি, যার নাম দেব Λ, মানে $\Lambda =$"". লক্ষ কর যে, কোনো কিছুর আগে বা পরে Λ জুড়লে কিছুই বদলাবে না। Λ-র এই ধর্মটাকেই নীচের উদাহরণে ব্যবহার করব।

Example 78: ধরো S হচ্ছে যাবতীয় binary string-এর set, যাদের দৈর্ঘ্য ≥ 0. এর উপর binary operation-টা নিলাম $\bullet$, মানে একটার পর একটা জুড়ে দেওয়া। তাহলে $(S, \bullet)$ একটা monoid হবে, যেখানে identity-র ভূমিকা পালন করবে Λ-টা। ■

Example 79: True or false: S is the set of real 2×2 matrices and binary operation $\circ$ is defined on S by

$$A \circ B = AB + BA,$$

for $A, B \in S$. Then $(S, \circ)$ is a semigroup.[2] **(2004)**

SOLUTION:

The result is false.

Associativity-র জন্য দরকার

$$\forall A, B, C \in S (A \circ B) \circ C = A \circ (B \circ C).$$

দুই দিককে একটু দলাইমলাই করে দেখা যাক। প্রথমে বাঁদিক--

$$\begin{aligned} (A \circ B) \circ C &= (AB + BA) \circ C \\ &= (AB + BA)C + C(AB + BA) \\ &= ABC + BAC + CAB + CBA. \end{aligned}$$

তারপর ডানদিক--

$$\begin{aligned} A \circ (B \circ C) &= A \circ (BC + CB) \\ &= A(BC + CB) + (BC + CB)A \\ &= ABC + ACB + BCA + CBA. \end{aligned}$$

নাঃ, ঠিক একই জিনিস বলে তো বোধ হচ্ছে না! প্রথমের ABC আর শেষের CBA-টা মিলছে বটে, কিন্তু মাঝের দুটো term-এ A, B, C-গুলো আগেপরে হয়ে গেছে। সুতরাং নির্ঘাত commutativity-র অভাব নিয়ে একটা ঝামেলা বাঁধানো যাবে।

Take

$$A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}, B = \begin{bmatrix} 1 & 1 \\ 2 & 0 \end{bmatrix}, C = \begin{bmatrix} -2 & 3 \\ 1 & 2 \end{bmatrix}.$$

কী করে জানলাম যে এই matrix-গুলো দিয়ে কাজ চলবে? এর উত্তর হচ্ছে এই যে, এখনও মোটেই জানি না সত্যিই কাজ চলবে কি না। স্রেফ যা খুশী তিনটে matrix নিয়েছি। সাধারণতঃ খুব সোজা কোনো matrix না নিলে commutativity নিয়ে এমনিতেই ঝামেলা বাঁধে, তার জন্য আলাদা করে বিরাট কিছু চেষ্টা করতে হয় না। নেহাত যদি আমাদের দুর্ভাগ্যক্রমে ঝামেলা না বাঁধে, তবে কোনো একটা সংখ্যাকে একটু এদিক ওদিক করে দিলেই হবে। তবে বোধহয় তার দরকার হবে না। আমাদের কাজ হচ্ছে $(A \circ B) \circ C$ আর $A \circ (B \circ C)$ এ দুটোকে আলাদা করে বার করা। A, B, C-গুলো ঠিকঠাক নেওয়া হয়ে থাকলে এ দুটো আলাদা matrix হবে।
রাফে কষলেই দেখবে--

Then

$$A \circ B = \begin{bmatrix} 9 & 7 \\ 13 & 7 \end{bmatrix}$$

and so

$$(A \circ B) \circ C = \begin{bmatrix} 10 & 48 \\ 16 & 74 \end{bmatrix}$$

এবার $A \circ (B \circ C)$ বার করি--

But

$$B \circ C = \begin{bmatrix} 3 & 3 \\ 1 & 7 \end{bmatrix}$$

and so

$$A \circ (B \circ C) = \begin{bmatrix} 17 & 35 \\ 35 & 67 \end{bmatrix} \neq (A \circ B) \circ C.$$

> So the operation is not associative. Hence $(S, \circ)$ cannot be a semigroup.

■

20.1 Semigroup থেকে group

এবার আমরা কিছু অংক দেখব যেগুলোর মূল ব্যাপারটা হল--একটা semigroup-এর উপর কিছু শর্ত চাপানো থাকবে, এবং তা থেকে দেখাতে হবে যে, semigroup-টা আসলে একটা group. অংকগুলো মূলতঃ কিছু কসরৎ ছাড়া কিছুই নয়। Modern algebra শেখার জন্য এদের বিরাট কোনো ভূমিকা নেই। যারা এই বইটা পরীক্ষা পাশের জন্য পড়ছ না, তারা স্বচ্ছন্দে এই অধ্যায়ের বাকি অংশটুকু খালি হাল্কা করে চোখ বুলিয়ে ছেড়ে দিতে পারো।

Example 80: Prove that any finite semigroup in which both the cancellation laws hold is a group. Is it true in case of an infinite semigroup? Justify.[4+1] **(1999,2002,2006,2013)**

SOLUTION: এই অংকটায় খানিকটা লড়াই করতে হবে। প্রথমে দেখে নিই যে কী দেওয়া আছে--

> Given: G is a finite semigroup such that the left cancellation law holds:
>
> $$\forall a, b, x \in G \quad (xa = xb \implies a = b),$$
>
> and the right cancellation law holds:
>
> $$\forall a, b, x \in G \quad (ax = bx \implies a = b).$$

লক্ষ কর যে, cancellation law দুটোকে বিশদ করে লিখে নিলাম। এতে পরে মাথা গুলিয়ে যাবার সম্ভাবনা কম থাকে। এবার লিখি কী দেখাতে হবে--

> To show that G is a group,

যেহেতু G একটা semigroup আছেই, তার মানে দেখাতে হবে খালি--

> ie, G has identity and every element has inverse in G.

আমরা গত অধ্যায়ে "Finite set-এর মজা" আলোচনা করার সময়ে শিখেছিলাম যে যদি $f : S \to S$ হয় যেখানে S একটা finite set, তবে f-এর পক্ষে one-one হওয়া, onto হওয়া এবং bijection হওয়া সমার্থক। এদের মধ্যে একটা হলেই অন্য দুটোও হতে বাধ্য। এবার সেটা কাজে লাগবে।

> Identity:
>
> We pick any $a \in G$. (Possible $\because G$ is a semigroup, $\therefore G \neq \phi$.)
>
> Define a function $f : G \to G$ as $f(x) = ax$.
>
> Then f is one-one.
>
> ⟦ Because:
>
> $$f(x) = f(y) \implies ax = ay \implies x = y,$$
>
> by the left cancellation law.
>
> ⟧

Since G is finite, f must also be onto.

এই ধাপটাই এই অংকের সবচেয়ে কঠিন ধাপ। এখানেই G-এর finiteness কাজে লাগল।

$\therefore \exists e \in G \quad f(e) = a$, ie,

$$ae = a. \qquad (*)$$

এবার দেখাব যে, এই e-টাই identity হবে। আমরা আপাততঃ খালি দেখিয়েছি যে, কোনো একটা <u>বিশেষ</u> a-র জন্য $ae = a$ হয়। সুতরাং প্রথম কাজ এটা দেখানো যে, এই বিশেষ a-টার জন্য $ea = a$-ও হয়।

Multiplying from the right by a,

$$aea = aa,$$

and applying left cancellation law,

$$ea = a. \qquad (**)$$

এবার $\forall g \in G$-এর জন্য দেখাব যে $ge = eg = g$.

Shall show that e is the identity of G, ie,

$\forall g \in G \quad eg = ge = g.$

$\forall g$ Take any $g \in G$.

Then multiplying $(**)$ by g from left,

$$gea = ga,$$

and so by cancelling a from the right,

$$ge = g,$$

as required.

Similarly, using $(*)$, we get $eg = g$, as required.

এবার inverse দেখানোর পালা--

<u>Inverse:</u>

To show

$\forall g \in G \quad \exists h \in H \quad gh = hg = e.$

$\forall g$ Take any $g \in G$.

Define a function $F : G \to G$ as $F(x) = gx$.

Then as before F is 1-1 and hence onto, because G is finite.

$\therefore \exists h \in G \quad F(h) = e$, ie, $gh = e$.

$\boxed{\exists h}$ Choose this $h \in G$.

এবার দেখাব $hg = e$.

Multiplying by g from the right,

$$ghg = eg = g = ge.$$

Cancelling g from the left,

$$hg = e,$$

as required.

এবার দ্বিতীয় অংশ--

No, this result does not hold in an infinite semigroup.

For example, take the semigroup S of all strings (of positive length) made of 0's and 1's under the concatenation operator.

এই semigroup-টার আলোচনা আমরা আগেও করেছি। এর সদস্যরা হল কিছু 0 আর 1 পরপর বসিয়ে তৈরী, যেমন--“0101”, “0”, “111111”, ইত্যাদি। Operation-টা হল concatenation অর্থাৎ একটার পর একটা জুড়ে দেওয়া, যেমন

“101”•“0000”= “1010000”>

লক্ষ কর যে দুটো element মিলিয়ে যে নতুন element-টা পাব সেটা সবসময়েই মূল element-দুটোর থেকে বেশী লম্বা হবে।

Since concatenation always increases the length of the string, S does not have an identity element.

■

Exercise 45: Prove that any finite semigroup in which both the cancellation laws hold, is a group. Show that the result fails in case of an infinite semigroup.[4+1] **(2009.3a)**
HINT:
আগের অংকটাই। ■

Exercise 46: Prove that a finite semigroup in which both the cancellation laws hold is a group. Does the theorem hold if the semigroup is infinite? Justify your answer.[5] **(2011.16)**
HINT:
একই অংক আবার একটু অন্য ভাষায়। ■

এবার একটা অন্য স্বাদের অংক।

Example 81: In a semigroup $(S, \bullet)$ if the equations $a \bullet x = b$ and $y \bullet a = b$ have solutions in S for x and y in S, then prove that $(S, \bullet)$ is a group. Here $a, b \in S$.[5] **(2001)**
SOLUTION:

Given that $(S, \bullet)$ is a semigroup and

$$\forall a, b \in S \quad \exists x, y \in S \quad a \bullet x = b, \;\; y \bullet a = b. \qquad (*)$$

ভালো করে বুঝে নাও যে, এটা আসলে প্রশ্নের শর্তটাই।

To show that S is a group.

Step 1: Shall show that $(S, \bullet)$ has an identity element.

প্রথমে দেখাব যে left identity আর right identity আছে। সেখান থেকে identity-তে পৌঁছব। Left identity মানে এমন একটা element যাকে দিয়ে কাউকে বাঁদিক থেকে গুণ করলে কিছুই বদলায় না। একইভাবে right identity দিয়ে ডানদিক থেকে গুণ করলে কিছুই বদলায় না।

Since S is a semigroup, so $S \neq \phi$.

So we can pick some $s \in S$.

Then, taking $a = b = s$ in (*),

$$\exists x, y \in S \quad s \bullet x = s \text{ and } y \bullet s = s.$$

এবার আমরা দেখাব যে, আসলে x একটা right identity এবং y একটা left identity.

Now, x is a right identity.

⟦ Because:

Take any $t \in S$.
Taking $a = s$ and $b = t$ in (*), we have $t = u \bullet s = s \bullet v$ for some $u, v \in S$.
So $t \bullet x = u \bullet s \bullet x = u \bullet s = t$.

⟧

Similarly, y is a left identity.

এবার দেখাব যে, আসলে $x = y$, ফলে এটা একাধারে left identity এবং right identity দুইই, সুতরাং এটাই identity.

So

$$\begin{aligned} x &= yx \quad [\because y \text{ is a left identity.}] \\ &= y \quad [\because x \text{ is a right identity.}] \end{aligned}$$

Thus $x = y = e$, say, is both a left and a right identity, and hence the identity element.

এবার inverse-এর পালা--

> Step 2: Shall show that every element $t \in S$ has inverse in S.

এখানেও left inverse আর right inverse আলাদা করে দেখিয়ে শুরু করব--

> Then, by taking $a = t$ and $b = e$ in (*),
>
> $$\exists p, q \in S \quad t \bullet p = e \text{ and } q \bullet t = e.$$

সুতরাং p হল একটা right inverse, আর q হল একটা left inverse. এবার দেখাব যে, এরা আসলে সমান--

> We have $p = q$.
>
> ⟦ Because:
>
> $$\begin{aligned} q &= q \bullet e \\ &= q \bullet t \bullet p \quad [\because e = t \bullet p] \\ &= e \bullet p \quad [\because e = q \bullet t] \\ &= p. \end{aligned}$$
>
> ⟧
>
> Thus $p = q$ is both a left and a right inverse, and hence is the inverse of t.

■

Example 82: $(S, \bullet)$ is a semigroup. Show that $(S, \bullet)$ will form a group if $a \bullet x = b$ and $y \bullet a = b$ have (unique) solutions in S for any two $a, b \in S$. Apply this to show that the semigroup of 2×2 real matrices under matrix multiplication does not form a group.[4+1] **(2004)**

SOLUTION: প্রথম অংশ আগের মতই। এখানে "unique" শব্দটার আসলে কোনো প্রয়োজন নেই।
দ্বিতীয় অংশটায় একটা logic-এর ভুল আছে। এখানে আমাদেরকে কোনো একটা কিছুকে group নয় দেখাতে বলেছে। এবং সেটা করতে বলেছে প্রথম অংশটাকে ব্যবহার করে। কিন্তু প্রথম অংশে যে শর্তটা দেওয়া ছিল, আমরা খালি দেখিয়েছি যে, সেটা হল group হবার একটা sufficient শর্ত, necessary তো দেখাই নি। তাই সেই শর্তটা ক্ষুণ্ণ হলেই "group হবে না" এমনটা জোর দিয়ে আমরা বলতে পারি না। ঠিক যেন প্রথম অংশে দেখিয়েছি "পাখীরা উড়তে পারে", আর দ্বিতীয় অংশে বলছে যে "আরশোলা পাখী নয়", এবং তা থেকে সিদ্ধান্ত করতে বলছে যে, "আরশোলা উড়তে পারে না"। সেটা করা যায় না।
যাই হোক, এখানে আসলে প্রথম অংশের শর্তটা group হবার জন্য necessary-ও বটে, যদিও সেটা প্রথম অংশে দেখাতে বলে নি। কারণ, একটা group-এর মধ্যে $a \bullet x = b$ হলে সেটাকে সব সময়েই solve করে পাওয়া যাবে $x = a^{-1} \bullet b$. একইভাবে $y \bullet a = b$-এর সমাধান হবে $y = b \bullet a^{-1}$. সংক্ষেপে এই কথাটা লিখে ভুল অংকটাকে মেরামত করার চেষ্টা করি--

> Second part : We observe that the condition in the first part is also necessary for $(S, \bullet)$ to be a group.

ওড়ার উপমা দিয়ে ভাবলে necessary শর্ত হল এরকম--"যারা উড়তে পারে তাদের পাখা থাকে।" এবার যদি দেখাতে পারি যে, "খরগোশের পাখা নেই" অমনি সিদ্ধান্ত করতে পারব যে, "খরগোশ উড়তে পারে না"।

তার মানে আমাদের অংকে এবার এমন দুটো matrix a, b জোগাড় করতে হবে যাতে $ax = b$-এর কোনো solution না থাকে। মানে যাই matrix x নাও না কেন a-কে তা দিয়ে গুণ করে কোনোভাবেই b পাবার জো নেই! এরকম একটা সহজ উদাহরণ হবে যদি a নিই zero matrix, আর b নিই যা খুশী একটা nonzero matrix. শূন্যকে গুণ করে তো আর nonzero বানানো যাবে না!

> Taking
>
> $$a = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \text{ and } b = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix},$$
>
> we see that we cannot have any matrix x such that $ax = b$, because for any x the matrix ax must be the zero matrix, but b is nonzero. So the semigroup of 2×2 real matrices under matrix multiplication does not form a group.

■

Exercise 47: $(G, \bullet)$ is a semigroup. For all $a, b \in G$ the equations $ax = b$ and $ya = b$ have solutions in G. Show that $(G, \bullet)$ is a group. Apply this to show that the semigroup of 2×2 real matrices of the form

$$\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}$$

under matrix multiplication does not form a group.[4+1] **(2007)**

HINT:

আগের অংকটাই, সামান্য অন্য ভাষায়। ■

Example 83: Let $(S, \circ)$ be a semigroup. If for all $x, y \in S$, $x^2 \circ y = y = y \circ x^2$, prove that $(S, \circ)$ is an Abelian group.[3] **(2005)**

SOLUTION:

> Given: $(S, \circ)$ is a semigroup with
>
> $$\forall x, y \in S \quad y \circ x^2 = x^2 \circ y = y. \qquad (*)$$

শর্তটার দিকে তাকালেই বুঝবে যে, এখানে x^2-টা identity-র ভূমিকা পালন করছে। কিন্তু x-এর আগে তো $\forall$ আছে, মানে x যা খুশি হতে পারে। সুতরাং আন্দাজ করতে পারছ যে, এখানে সবার *square*-ই হল identity-র সমান। মানে $\forall x \in S \quad x^2 = e$. এই শর্ত হলে যে Abelian হয়, সেটা আমরা এই অধ্যায়ের গোড়ার একটা অংকে শিখেছিলাম। সেই যুক্তিটাই মোটামুটিভাবে এখানেও খাটবে।

> To show: $(S, \circ)$ is an Abelian group.
>
> Step 1: Shall show $(S, \circ)$ has an identity element, ie,
>
> $\exists e \in S \quad \forall y \in S \quad y \circ e = e \circ y = y.$

আমরা তো আন্দাজ করে ফেলেইছি যে, যা খুশি একটা x নিয়ে তার square করে দিলেই identity পাওয়া যাবে--

> $\because (S,\circ)$ is a semigroup, $\therefore S \neq \phi$.
>
> $\therefore$Can pick some $x \in S$.
>
> $\exists e$ Choose $e = x^2$.
>
> $\forall y$ Take any $y \in S$.
>
> Then, by (*),
> $$y \circ e = e \circ y = y,$$
> as required.
>
> Step 3: Since $\circ$ is associative, so it must have unique identity element.
>
> So we have
> $$\forall x \in S \quad x^2 = e. \qquad (**)$$
> This means every element is its own inverse.

ব্যস্, inverse দেখানোও হয়ে গেল!

> So the semigroup $(S,\circ)$ is a group.

এবার Abelian দেখাতে হবে। লক্ষ কর এই group-এ সবাই নিজেই নিজের inverse. এই কথাটা ব্যবহার করেই Abelian প্রমাণ করব।

> Abelian:
>
> Take any $x, y \in S$.
>
> Then, $xy = (xy)^{-1} = y^{-1}x^{-1} = yx$, as required.

■

Exercise 48: Prove that a semigroup $(G,\circ)$ is a non-commutative group where

$$G = \{(a,b) \in \mathbb{Q} \times \mathbb{Q} \ : \ a \neq 0\}$$

and the composition $\circ$ is defined by

$$(a,b) \circ (c,d) = (ac, ad+b) \text{ for } (a,b),(c,d) \in G.$$

[$\mathbb{Q}$ is the set of all rational numbers.☐] **(2014.18a)**
HINT: এটা আসলে Example 30 অংকটারই রূপভেদ। খালি এখানে বাড়তি বলে দিয়েছে যে, $(G,\circ)$ একটা semigroup. তাই closure আর associativity দেখাতে হবে না, কেবল identity আর inverse দেখালেই চলবে। ■

Answers

1. "ডাইনে মুড়": $N \mapsto E, \quad E \mapsto S, \quad S \mapsto W, \quad W \mapsto N$. "পিছে মুড়":

$N \mapsto S, \quad E \mapsto W, \quad S \mapsto N, \quad W \mapsto E.$ "হল্ট": $N \mapsto N, \quad E \mapsto E, \quad S \mapsto S, \quad W \mapsto W.$ **2.** বাঁয়। **4.** হবে, হবে, না, হবে। **5.** **(1)** closed, **(2)** closed, **(3)** closed, **(4)** closed নয়।
6. প্রথম জনের যুক্তি ঠিক। Closed দেখানোর জন্য দেখাতে হবে

$$\forall a, b \in \mathbb{N} \quad a \star b \in \mathbb{N}.$$

এখানে $\forall$ আছে, তাই এমন যুক্তি দিতে হবে যেটা যাবতীয় $a, b \in \mathbb{N}$-এর জন্যই খাটে। খালি একটা বিশেষ উদাহরণ নিয়ে ছেড়ে দিলেই চলবে না। কিন্তু যদি closed নয় দেখাতে চাও, তবে দেখাতে হবে

$$\exists a, b \in \mathbb{N} \quad a \star b \notin \mathbb{N}.$$

এখানে $\exists$ নিয়ে কাজ করছি, তাই একটা উদাহরণ দেখাতে পারাই যথেষ্ট। **7.** বিয়োগ commutative নয়, গুণ commutative. **8.** না, কারণ $r(f_1(1)) = r(1) = 2$, কিন্তু $f_1(r(1)) = f(2) = 3 \neq r(f_1(1))$.
10. **(1)** হ্যাঁ, $(1, 1)$. **(2)** না। **(3)** হ্যাঁ, $(0, 1)$. **11.** "পিছে" নিজেই! **12.** $1 \div (2 \div 4) \neq (1 \div 2) \div 4$.
13. $a \star b = a^b$. এখানে $(2 \star 3) \star 2 = (2^3)^2 = 8^2 = 64$, কিন্তু $2 \star (3 \star 2) = 2^{3^2} = 2^9 = 512$.
15. **(1)** Identity নেই। **(2)** 1-এর inverse নেই। **(3)** Closure নেই। **(4)** Associative নয়। **16.**

	ϕ	$\{1\}$	$\{2\}$	$\{1,2\}$
ϕ	ϕ	$\{1\}$	$\{2\}$	$\{1,2\}$
$\{1\}$	$\{1\}$	ϕ	$\{1,2\}$	$\{2\}$
$\{2\}$	$\{2\}$	$\{1,2\}$	ϕ	$\{1\}$
$\{1,2\}$	$\{1,2\}$	$\{2\}$	$\{1\}$	ϕ

17. সমীকরণের দুপাশেই ডানদিকে b^{-1} দিয়ে গুণ করে দাও। **20.** হ্যাঁ। **21.** হ্যাঁ। যে কোনো $n \in \mathbb{Z}$. **23.** $4, 1$. **24.** 3. **25.** 0-র order হল 1. **26.** 6. **27.** 16. **28.** 101. **34.** ঠিক। **35.** ভুল। সমবাহু ত্রিভুজ ঘুরিয়ে ফিট করার group-টা non-Abelian ছিল। কিন্তু ওর মধ্যে $H = \{e, f_1\}$ একটা nontrivial subgroup, যেটা Abelian. **38.** হ্যাঁ। **39.** তুমি কি করে পেলে $e_1 \in H$? এটা যতক্ষণ না পাচ্ছ, ততক্ষণ তো তুমি e_1-কে H-এর একটা identity বলে দাবী করতে পারো না! **42.** হ্যাঁ, $\mathbb{N}$ অবশ্যই closed under $+$. না, $(\mathbb{N}, +)$ একটা group নয়। হ্যাঁ, finite হওয়াটা দরকারী ছিল।

Chapter III
Group theory (year 2)

DAY 1
Coset

এবার আমরা একটা গুরুত্বপূর্ণ theorem শিখব যাকে বলে Lagrange's theorem (Lagrange-এর উচ্চারণ হল লাগ্রাঞ্জ)। এই theorem-টাকে দুটো দৃষ্টিকোণ থেকে দেখা যায়--এক, coset (কোসেট) বলে একটা জিনিসের দৃষ্টিকোণ থেকে, আর দুই, equivalence relation-এর দৃষ্টিকোণ থেকে। আমরা প্রথমে coset-এর দৃষ্টিকোণ থেকে শুরু করব। তার জন্য গোড়ায় জানা দরকার coset জিনিসটা কী।

1.1 Coset কাকে বলে?

আমরা জানি যে, G যদি একটা group আর H তার একটা subgroup হয়, তবে H অবশ্যই G-এর একটা subset হবে। সাধারণতঃ subset ভাবতেই আমাদের মনে যে চিত্রটা ভেসে ওঠে, সেটা হল Fig 1-এর মত। কিন্তু আমরা এক্ষুণি দেখব যে, subgroup-এর ক্ষেত্রে চিত্রটা Fig 1-র চেয়ে বরং Fig 2-এর বেশী কাছাকাছি। এখানে group-টা যেন এক প্যাকেট পাঁউরুটি, আর subgroup-টা তার মধ্যে একটা স্লাইস্। Subgroup-টা ছাড়াও পাশাপাশি অনেকগুলো একই আকারের স্লাইস্ সাজানো আছে, এই সব স্লাইস্ নিয়েই পুরো group-টা তৈরী। কোথা থেকে এই স্লাইস্গুলোর উৎপত্তি হল, সেই আলোচনা থেকেই আমরা Lagrange's theorem-এ গিয়ে পৌঁছব। প্রথমে আমরা ব্যাপারটাকে কিছু উদাহরণ দিয়ে বুঝব। এখানে বলে রাখা ভালো যে, অংকের ভাষায় স্লাইস্গুলোকে বলে এককেটা **coset.**

Example 1: আমাদের প্রথম উদাহরণে আমরা কাজ করব অতিপরিচিত group $G = (\mathbb{Z}, +)$ নিয়ে। $\mathbb{Z}$ মানে যাবতীয়

Fig 1

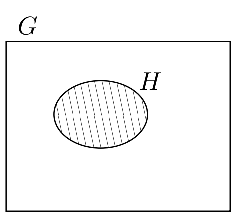
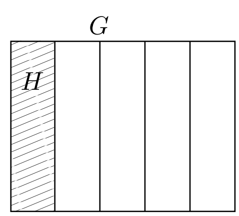


Fig 2



integer-এর set. এটাকে আমরা সাজিয়ে লিখব এইভাবে--

$$\begin{array}{ccc} \vdots & \vdots & \vdots \\ -6 & -5 & -4 \\ -3 & -2 & -1 \\ 0 & 1 & 2 \\ 3 & 4 & 5 \\ 6 & 7 & 8 \\ \vdots & \vdots & \vdots \end{array}$$

এখানে যাবতীয় integer-দের তিনটে column-এ লিখেছি। প্রথম column-এ আছে সেইসব সংখ্যা যারা 3 দিয়ে ভাগ যায়, দ্বিতীয় সারিতে আছে তারা যাদের 3 দিয়ে ভাগ করলে ভাগশেষ হয় 1. শেষের সারির সদস্যদের ক্ষেত্রে ভাগশেষ হয় 2. লক্ষ কর প্রথম সারিটা একটা subgroup. এটা বোঝার সবচেয়ে সহজ উপায় হল এটা দেখা যে, প্রথম সারির যেকোনো দুটো সংখ্যার বিয়োগফল সেই সারিতেই আছে (কারণ দুটো সংখ্যা 3 দিয়ে ভাগ গেলে, তাদের বিয়োগফলও 3 দিয়ে ভাগ যেতে বাধ্য!)। এই subgroup-টার নাম দেওয়া যাক H, মানে $H = 3\mathbb{Z}$. কিন্তু বাকিদুটো column-এর কোনোটাই subgroup নয়। যেমন দ্বিতীয় column-এ আছে -5, -2. কিন্তু এদের বিয়োগফল $-5-(-2) = -3$ মোটেই দ্বিতীয় column-এ নেই! একইভাবে 2 আর 8 আছে তিন নম্বর column-এ কিন্তু তাদের বিয়োগফল $2-8=-6$ পড়েছে তিন নম্বর column-এর বাইরে।

একটু আগে যে পাঁউরুটির স্লাইসের কথা বলছিলাম, এই উদাহরণের সঙ্গে তা মিলিয়ে দ্যাখো। এখানে $\mathbb{Z}$ হল পুরো প্যাকেটটা, তার মধ্যে H রয়েছে একটা স্লাইসের মত। মোট তিনটে স্লাইস্ (মানে coset) আছে। প্রথম coset-টা তো H নিজেই। বাকী দুটো coset-এর জন্যও এই H থেকেই। সেটা বোঝার জন্য প্রথমে H-এর বাইরে যেকোনো একটা সংখ্যা নাও, যেমন 1. এইবার H-এর সব সংখ্যার সাথে 1 যোগ করে দিলেই দ্বিতীয় সারির সংখ্যাদের পাওয়া যাবে। তাই আমরা দ্বিতীয় সারিটাকে $1+H$ হিসেবে লিখতে পারি। এবার প্রথম দুই সারিতে নেই এমন যেকোনো একটা সংখ্যা নাও, যেমন 2. লক্ষ কর $2+H$ হচ্ছে তৃতীয় সারি। অংকের ভাষায় আমরা বলব-- H subgroup-টার তিনটে coset:

$$H, \quad 1+H, \quad 2+H.$$

এখানে দ্বিতীয় সারিটাকে যে আমরা $1+H$ লিখেছিলাম, সেখানে 1-টা কিন্তু গুরুত্বপূর্ণ নয়, দ্বিতীয় সারি থেকে অন্য যেকোনো সংখ্যা নিলেও একই কাজ চলত। যেমন যদি 4 নিতাম, তবে আমরা দ্বিতীয় সারিটাকে $4+H$-ও লিখতে পারতাম। পরীক্ষা করে দ্যাখো--প্রথম সারির যে কোনো সংখ্যার সাথে 4 যোগ করলে তুমি দ্বিতীয় সারির একটা সংখ্যা পাবে, এবং বিপরীতপক্ষে দ্বিতীয় সারির যে কোনো সংখ্যাকেই প্রথম সারির কোনো সংখ্যার সঙ্গে 4 যোগ করে পাওয়া যায়। ■

Exercise 1: একইভাবে পরীক্ষা করে দ্যাখো যে, $2+H$ আর $5+H$ আসলে একই। বল তো $10+H$ কোন সারিটাকে বোঝাচ্ছে? ■

লক্ষণীয় যে, স্লাইস্‌গুলো (মানে coset-গুলো) সকলেই সমান সাইজের, কারণ সকলেই তো আসলে H থেকেই তৈরী। এই কথাটা আরো স্পষ্ট হবে একটা finite group-এর উদাহরণ নিলে।

Example 2: এবার আমরা নেব $G = (\mathbb{Z}_8, \oplus)$ আর subgroup-টা নেব $H = \{0, 4\}$. মনে আছে নিশ্চয়ই $\mathbb{Z}_8$-এর সদস্যরা হল $\{0, 1, 2, ..., 7\}$, আর $\oplus$ হল "যোগ করে 8 দিয়ে ভাগ করে ভাগশেষ নেওয়া"। যেমন $3 \oplus 6 = 1$, কারণ $3+6=9$-কে 8 দিয়ে ভাগ করলে ভাগশেষ হয় 1.

এবার তবে G-এর মধ্যে H-এর coset-দের পরিচয় নেওয়া যাক। এখানে H হল পাঁউরুটির প্রথম স্লাইস্। সুতরাং আমাদের মনে $\mathbb{Z}_8$-এর চিত্রটা আপাততঃ Fig 3-এর (a)-র মতন। এবার এই স্লাইস্‌টার (মানে coset-টার) বাইরে যে কোনো একটা element নাও, যেমন 6. তাহলে পরের coset-টা পাব

$$6 \oplus H = 6 \oplus \{0, 4\} = \{6 \oplus 0, 6 \oplus 4\} = \{6, 2\}.$$

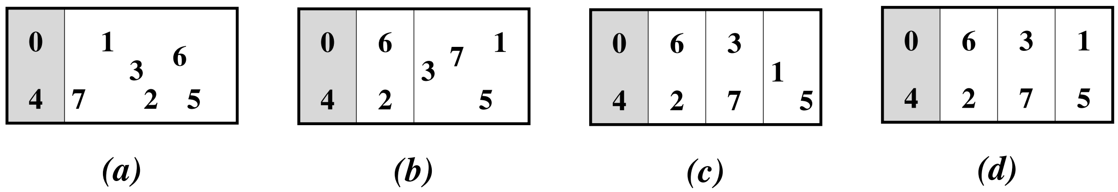


Fig 3

এই হল দ্বিতীয় স্লাইস (Fig 3(b))। এবার এমন একটা element নাও, যেটা এই দুটো coset-এরই বাইরে, যেমন 3. তাহলে আমাদের তৃতীয় coset-টা হবে

$$3 \oplus H = 3 \oplus \{0, 4\} = \{3 \oplus 0, 3 \oplus 4\} = \{3, 7\}.$$

পড়ে আছে খালি 1 আর 5. যদি এদের মধ্যে ধরো 1-টা নিই, তবে চতুর্থ coset-টা হবে

$$1 \oplus H = 1 \oplus \{0, 4\} = \{1 \oplus 0, 1 \oplus 4\} = \{1, 5\}.$$

আর কিছুই পড়ে নেই, তার মানে H-এর মোট এই চারটেই coset আছে। ■

লক্ষ কর--

- coset-গুলোর সব সমান সাইজ,
- এদের মধ্যে কোনো intersection নেই, অর্থাৎ " The cosets are mutually exclusive."
- group-এর সব element-ই কোনো না কোনো coset-এর মধ্যে আছে, অর্থাৎ " The cosets are mutually exhaustive."

যদি H-এর সাইজ হয় k (উপরের উদাহরণে $k = 2$ ছিল), তবে সবগুলো coset-এর সাইজই হবে k. যদি এরকম m-খানা coset নিয়ে group-টা তৈরী হয় (উদাহরণে $m = 4$ ছিল), তবে group-এর সাইজ হবে mk. তার মানে subgroup-এর সাইজ দিয়ে group-এর সাইজটা ভাগ যেতে বাধ্য। এই কথাটাই হল **Lagrange's theorem.** কাল আমরা এই theorem-টা গুছিয়ে লিখে প্রমাণ করব। আজকেটা কেটে যাবে coset-দের বিভিন্ন ধর্ম আলোচনা করতে।
এই প্রসঙ্গে notation নিয়ে দুটো কথা বলা দরকার--

- আমরা জানি, যে কোনো group-এই একটা binary operation থাকে। লেখার সময়ে এটাকে সাধারণতঃ যোগ-জাতীয় চিহ্ন (যেমন $a + b$ বা $a \oplus b$) অথবা গুণ-জাতীয় চিহ্ন (যেমন $a \star b$ বা ab) দিয়ে লেখা হয়। আমরা এতক্ষণ যোগচিহ্ন ব্যবহার করেছি। ফলে coset-গুলো দেখতে হয়েছে $a + H$-এর মতন। যদি গুণ ব্যবহার করতাম, তবে coset-গুলোকে লিখতাম $a \star H$ বা aH রূপে।
- আমাদের উদাহরণগুলোতে group-গুলো ছিল commutative, তাই aH এবং Ha-র মধ্যে কোনো তফাৎ ছিল না। এখানে aH মানে
$$aH = \{ah \ : \ h \in H\},$$
আর Ha মানে
$$Ha = \{ha \ : \ h \in H\}.$$
কিন্তু commutative না হলে aH আর Ha একই জিনিস নাও হতে পারে। তখন আমরা aH-কে বলব **left coset**, আর Ha-কে বলব **right coset.**

এবার আমরা সংজ্ঞাগুলো গুছিয়ে লিখে নিই।

> **DEFINITION: Left and right coset**
>
> Let G be any group, and let H be any subgroup of G. Then a **left coset** of H in G means any subset of G of the form
>
> $$aH = \{ah \ : \ h \in H\},$$
>
> where $a \in G$. Similarly, a **right coset** of H in G means any subset of G of the form
>
> $$Ha = \{ha \ : \ h \in H\},$$
>
> where $a \in G$.

Group-টা যদি Abelian হয়, তবে অবশ্য আলাদা করে left coset বা right coset বলার দরকার পড়ে না, খালি coset বললেই চলে।
এবার একটা non-Abelian উদাহরণ নিয়ে left এবং right coset-এর পার্থক্যটা বোঝা যাক। Non-Abelian group-এর উদাহরণ আমরা গত অধ্যায়েই একটা পেয়েছি--সেই ত্রিভুজের উদাহরণটা। সেটা নিয়েই কাজ করি।

Example 3: ত্রিভুজের উদাহরণে আমরা একটা সমবাহু ত্রিভুজকে কাগজে আঁকা একইরকম একটা ত্রিভুজাকৃতি ফ্রেমে কতভাবে ফিট করে বসানো যায় সেটাই দেখছিলাম। আমরা দেখেছিলাম কাজটা করা যায় মোট 6-ভাবে, এবং এই ছয়জনকে নিয়ে একটা group হয়--

$$G = \{e, r, \ell, f_1, f_2, f_3\}.$$

এর মধ্যে e হল identity, আর বাকিদের পরিচয় মনে পড়ে যাবে Fig 4 দেখে নিলেই। এই group-এর মধ্যে একটা subgroup হল $H = \{e, f_1\}$. এর left coset-গুলো কী কী? Right coset-গুলোই বা কী কী?
SOLUTION: প্রথমে left coset-গুলো বার করি। ধাপে ধাপে এগোব, Fig 5-এর দিকে চোখ রেখে। H নিজে তো অবশ্যই নিজের একটা left coset. এবার H-এর বাইরে G-এর যা খুশী একটা element নাও, ধরো r. তাহলে আরেকটা left coset পাবে--

$$rH = \{re, rf_1\} = \{r, f_2\},$$

কারণ $rf_1 = f_2$. এটা চট্ করে চোখে না পড়লে কাগজে করে মিলিয়ে দেখতে পারো।
যাই হোক, এই যে দুটো left coset পেলাম তাদের বাইরে, G-এর যা খুশী একটা element নাও, ধরো ℓ. তা থেকে নতুন আরেকটা left coset পাব--

$$\ell H = \{\ell e, \ell f_1\} = \{\ell, f_3\},$$

কারণ $\ell f_1 = f_3$. ব্যস্, এই তিনটে left coset-এর বাইরে G-এর আর কোনো element পড়ে নেই, সুতরাং এরাই হল G-এর মধ্যে H-এর যাবতীয় left coset.

Fig 4

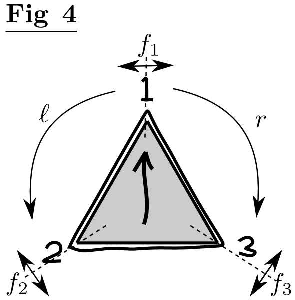
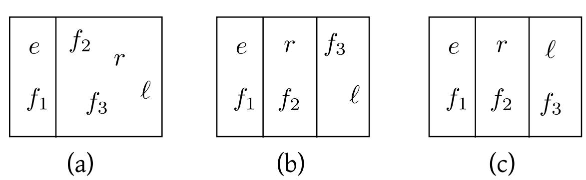


Fig 5



এবার right coset-গুলো বার করি। অবশ্যই H নিজেই নিজের একটা right coset. এর বাইরে যা খুশী একটা element নাও, ধরো r. তাহলে এই right coset-টা পাবে--

$$Hr = \{er, f_1 r\} = \{r, f_3\}.$$

কারণ ত্রিভুজটাকে নিয়ে একটু খেলা করলেই দেখবে যে $f_1 r = f_3$. এবার এই দুটো right coset-এর বাইরে যা খুশী একটা element নিই, ধরো, ℓ. তবে নতুন যে right coset-টা পাবে সেটা হল--

$$H\ell = \{e\ell, f_1\ell\} = \{\ell, f_2\},$$

কারণ $f\ell = f_2$.
লক্ষ কর, যাই left coset নাও আর যাই right coset নাও, দুই ক্ষেত্রেই G-কে ঠিক তিনটে স্লাইসে ভেঙে ফেলা গেল। দুই ক্ষেত্রেই H নিজে তাদের মধ্যে একটা স্লাইস। কিন্তু বাকি দুটো স্লাইস left coset-এর বেলায় একরকম, আর right coset-এর বেলায় অন্যরকম হল। ■

লক্ষ কর যে এই দুটো set-এর cardinality সমান, অর্থাৎ যতগুলো left coset আছে, ঠিক ততগুলোই right coset আছে। এই ব্যাপারটা খালি এই উদাহরণেই নয়, সব সময়েই হয়। সেটাই এই অংকে দেখাতে বলেছে।

Example 4: H is a subgroup of a group G. Prove that the set of all left cosets of H in G and the set of all right cosets of H in G have the same cardinality.[4] **(2011.8a)**
SOLUTION:

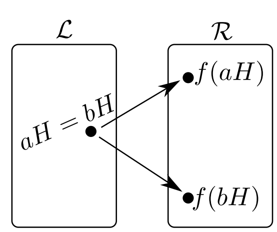
> Let $\mathcal{L}$ be the set of all left cosets of H in G.
> Similarly, let $\mathcal{R}$ be the set of all right cosets of H in G.

অর্থাৎ আমাদের উদাহরণে $\mathcal{L} = \{H, rH, r^2H\}$ এবং $\mathcal{R} = \{H, Hr, Hr^2\}$. দুটো set-এর cardinality সমান দেখানোর অমোঘ অস্ত্র হল ওদের মধ্যে একটা bijection দেখাতে পারা। আমরা সেই চেষ্টাই করব।

> Consider the map $f : \mathcal{L} \to \mathcal{R}$ given by $f(aH) = Ha^{-1}$.

প্রথমে দেখাতে হবে যে, এটা সত্যিই একটা well-defined function. পাছে এমন না আবার হয়ে যায় যে $aH = bH$, কিন্তু $f(aH) \neq f(bH)$. তবে Fig 6-এর মত এক জায়গা থেকে দুটো তীর চিহ্ন বেরিয়ে যাবে, যেটা কোনো function-এর ক্ষেত্রে হতে পারে না।

Fig 6



<u>Well-defined:</u> Shall show

$\forall a, b \in G \quad \big(aH = bH \implies Ha^{-1} = Hb^{-1}\big)$

$\forall a, b$ Take any $a, b \in G$ with $aH = bH$.

এবার দুটো set-কে সমান দেখাতে হবে--Ha^{-1} আর Hb^{-1}. কিন্তু আগে a আর b-এর মধ্যে একটা সম্পর্ক বার করে রাখলে সুবিধা হবে।

$\because a \in aH = bH$,
$\therefore a = bh$ for some $h \in H$.

এইবার দেখাব যে $Ha^{-1} \subseteq Hb^{-1}$.

Take any $\alpha \in Ha^{-1}$.
Then

$$\begin{aligned} \alpha &= xa^{-1} \quad [\text{ for some } x \in H.] \\ &= xh^{-1}b^{-1} \quad [\because a = bh] \\ &\in Hb^{-1} \quad [\because x, h \in H] \end{aligned}$$

$\therefore Ha^{-1} \subseteq Hb^{-1}$.

একইভাবে $Hb^{-1} \subseteq Ha^{-1}$.

Similarly, interchanging a and b, we have $Hb^{-1} \subseteq Ha^{-1}$.
So $Ha^{-1} = Hb^{-1}$, as required.

সুতরাং দেখানো শেষ হল যে, আমাদের f-টা সত্যিই well defined.
এরপর one-one দেখাতে হবে--

<u>One-one:</u> Shall show

$\forall a, b \in G \quad \big(f(aH) = f(bH) \implies aH = bH\big)$.

$\forall a, b$ Take any $a, b \in G$ with $f(aH) = f(bH)$.

আবার দুটো set-কে সমান দেখাতে হবে--aH আর bH. প্রথমে এবার $aH \subseteq bH$ দেখাব--

Take any $x \in aH$.

আমাদের উদ্দেশ্য হল $x \in bH$ দেখানো। তার জন্য a-কে b দিয়ে লিখতে পারলে সুবিধা হবে।

$\because f(aH) = f(bH)$, $\therefore Ha^{-1} = Hb^{-1}$.
$\therefore a^{-1} \in Hb^{-1}$, ie, $a^{-1} = hb^{-1}$ for some $h \in H$.
Hence $a = bh^{-1}$.

বাঃ, a-কে b দিয়ে লেখার একটা চমৎকার কায়দা পাওয়া গেল। এবার তাহলে $x \in bH$ দেখানোর চেষ্টা করি--

Then $x = ah_1$ for some $h_1 \in H$.
So $x = \underbrace{bh^{-1}}_{a} h_1 \in bH$.

একইভাবে, $bH \subseteq aH$-ও প্রমাণ হবে--

Similarly, interchanging a and b, we have $bH \subseteq aH$.
So $aH = bH$, as required.

বাকি থাকে onto দেখানো--

Onto: Shall show
$\forall x \in G \quad \exists y \in G \quad f(yH) = Hx$.
$\forall x$ Take any $x \in G$.
$\exists y$ Choose $y = x^{-1} \in G$.
Then $f(yH) = Hy^{-1} = Hx$, as required.

লম্বা প্রমাণ। একটু উপসংহারের ছলে মনে করিয়ে দিই কী দেখানোর কথা ছিল--

$\therefore f : \mathcal{L} \to \mathcal{R}$ is a bijection.
$\therefore \mathcal{L}$ and $\mathcal{R}$ have the same cardinality, as required.

■

একটা group-এর মধ্যে একটা subgroup-এর কতগুলো coset আছে সেই সংখ্যাটাকে বলে ওই group-এর মধ্যে ওই subgroup-টার **index.** সংজ্ঞাটা গুছিয়ে লিখে রাখি--

DEFINITION: Index of a subgroup

Let H be any subgroup of a group G. Then the **index** of H in G is defined as the number of left cosets (or right cosets) of H in G. It is denoted by $[G : H]$. If there are infinitely many cosets, then the index is defined to be ∞.

পাঁউরুটির স্লাইসের উপমাটা ভাবলেই বুঝবে নীচের theorem-টা কেন ঠিক--

THEOREM

For any finite group G and any subgroup H of G we have

$$[G : H] = |G|/|H|.$$

1.2 পাঁউরুটির স্লাইসের প্রমাণ

এতক্ষণ যা যা আলোচনা করলাম, তা থেকে একটা কথা কিন্তু স্পষ্ট হয়নি--H-টা যে একটা subgroup সেটা কোথায় কাজে লাগল? H তো G-এর যে কোনো একটা subset হলেই চলত বলে মনে হচ্ছে। কিন্তু না, আমরা যেভাবে coset-গুলো তৈরী করছি, সেটা যে কোনো subset-এর বেলায় করা যেত না। যেমন নীচের উদাহরণে।

Example 5: ধরো আবার $G = (\mathbb{Z}_8, \oplus)$ নিই। আগে $H = \{0, 4\}$ নিয়েছিলাম, যেটা একটা subgroup ছিল। এবার ধরো $H = \{0, 7\}$ নিলাম, যেটা একটা subgroup নয় কারণ $7 \oplus 7 = 6 \notin H$. এবার তাহলে H-এর বাইরে যা খুশী একটা element নিই, ধরো 1. তাহলে একটা coset হওয়া উচিত

$$1 \oplus H = \{1 \oplus 0, 1 \oplus 7\} = \{1, 0\}.$$

কিন্তু এটা তো একটা নতুন স্লাইস হতে পারে না, কারণ 0 তো আগেই H-এর মধ্যে ঢুকে গেছে! ■

সুতরাং যদি আমরা যে কোনো subset H নিয়ে coset বানানোর মত করে এগোই তবে যাদের পাব তারা একজনের ঘাড়ে একজন উঠে পড়তে পারে। কিন্তু H যদি একটা subgroup হয়, তবে সে সমস্যা কখনোই হবে না, এবং পাঁউরুটির স্লাইসের উপমাটা অক্ষরে অক্ষরে খাটবে। এইবার সেটাই আমরা বিভিন্ন অংকের মধ্যে দিয়ে প্রমাণ করব।

Example 6: True or false? Justify. Any two left cosets of a subgroup of a group are either disjoint or the same.[2] **(2004)**

SOLUTION: দেখাতে বলেছে, হয় disjoint অথবা same. এরকম "এটা অথবা ওটা" জাতীয় জিনিস দেখানোর একটা কায়দা হল, দুটোর মধ্যে যে কোনো একটা নয় ধরে নিয়ে অন্যটাকে দেখানো। এখানে আমরা disjoint নয় ধরে নিয়ে same দেখাব।

> We shall prove that the statement is true.
> Let G be a group, and H be a subgroup.
> Let $a, b \in G$ with $aH \cap bH \neq \phi$.

Disjoint ধরে নিলাম, এবার same দেখাব।

> Shall show that $aH = bH$.

এর জন্য যথারীতি $aH \subseteq bH$ আর $bH \subseteq aH$ দেখাব। কিন্তু আগে a আর b-এর মধ্যে একটা সম্পর্ক বার করে রাখি--

> We can pick some $c \in aH \cap bH$.
> Then $c = ah_1 = bh_2$ for some $h_1, h_2 \in H$.
> Thus,
> $$a = bh_2h_1^{-1} \text{ and } b = ah_1h_2^{-1}.$$

∎

এইবার $aH \subseteq bH$ দেখানো শুরু করছি।

> Take any $d \in aH$.
> Then $d = ah$ for some $h \in H$. So $d = bh_2h_1^{-1}h$.
> Since $h_1, h_2, h \in H$ so $h_2h_1^{-1}h \in H$. Hence $d \in bH$.
> $\therefore aH \subseteq bH$.

উল্টোদিকটা এতই একইরকম যে আলাদা করে লিখব না--

> Similarly, interchanging a and b, $bH \subseteq aH$.
> $\therefore aH = bH$, as required.

∎

এই অংকটা ছিল left coset-দের নিয়ে। ঠিক একই যুক্তি খাটে right coset-দের বেলাতেও। যুক্তিটা তোমার মাথায় ঠিকমত ঢুকেছে কিনা, সেটা প্রমাণ হয়ে যাবে right coset-দের দিয়ে নীচের অংকটা করতে পারলে।

Exercise 2: Show that any two right cosets of a subgroup of a group are either disjoint or the same. ∎

আগের অংকটায় প্রমাণ হল যে, স্লাইস্‌গুলো একটা আরেকটার ঘাড়ে উঠে পড়তে পারে না। এবার দেখাব যে, স্লাইস্‌গুলো সবাই সমান সাইজের।

Example 7: Prove that any two left cosets of H in a group G have the same number of elements.[2] **(2010.8b)**

SOLUTION: দুটো set-এর সাইজ সমান দেখানোর একটা কায়দা হল ওদের মধ্যে একটা bijection আছে দেখানো।

> Shall show that there is a bijection between H and any left coset of H in G.
> Take any left coset aH.
> Consider the function $f : H \to aH$ defined as $f(h) = ah$.

এবার দেখাব যে, এই f-টা একটা bijection, অর্থাৎ one-one এবং onto.

> This f is one-one.
>
> [[Because:
>
> If $f(h_1) = f(h_2)$, then $ah_1 = ah_2$, and so $h_1 = h_2$, by cancelling a.
>
>]]
>
> Also, f is onto.

⟦ Because:

If $b \in aH$ then $b = ah$ for some $h \in H$. So $b = f(h)$.

⟧

ব্যস্, bijection দেখানো শেষ।

Hence each left coset has the same size as H.

So all the left cosets have the same size, as required.

■

Exercise 3: Let $(H, \bullet)$ be a subgroup of $(G, \bullet)$. Show that two left cosets of H in G are either disjoint or identical. If $o(G) = n$ is finite then show that any two left cosets of H in G have the same number of elements.[5] **(2007)**

HINT: আগের দুটো মিলিয়ে তৈরী এই অংকটা। এখানে বাড়তি যে finite হওয়ার শর্তটা দিয়েছে, সেটার কোনো দরকার নেই। ■

অবশেষে আমরা Lagrange's theorem প্রমাণ করার জায়গায় পৌঁছেছি। সেটাই হবে আমাদের কালকের আলোচ্য বিষয়।

DAY 2
Lagrange's theorem

আগেই বলেছি যে, Lagrange's theorem প্রমাণ করা যায় দুই দৃষ্টিকোণ থেকে--coset-এর দৃষ্টিকোণ থেকে, আর eqivalence relation-এর দৃষ্টিকোণ থেকে। আমরা প্রথমে coset-এর দিক থেকে এগোব।

2.1 Coset ব্যবহার করে প্রমাণ

Example 8: State and prove Lagrange's theorem for a finite group.[2+4] **(1997,1999,2001,2003)**

SOLUTION:

Lagrange's theorem

Let G be any finite group, and let H be any subgroup of G. Then order of H must divide order of G.

এর প্রমাণ বস্তুতঃ গতকালের অংকগুলোর মধ্যেই করা হয়ে গেছে। তবে এখানে পুরো জিনিসটা একটু সংক্ষেপে গুছিয়ে লিখব, যাতে প্রমাণটা খুব লম্বা না হয়ে যায়।

Proof:

Step 1: Every element of G is in some left coset, because $\forall a \in G \quad a \in aH$.

∎

সুতরাং mutually exhaustive দেখানো শেষ! এবার mutually exclusive দেখাব--

Step 2: Any two distinct left cosets aH and bH must be disjoint.

⟦ Because:

Let, if possible, $ah_1 = bh_2$ for some $h_1, h_2 \in H$,
then $a = bh_2h_1^{-1}$ and $b = ah_1h_2^{-1}$.
So $\forall h \in H$

$$ah = bh_2h_1^{-1}h \in bH \quad (\because h_2h_1^{-1}h \in H),$$

and

$$bh = ah_1h_2^{-1}h \in aH \quad (\because h_1h_2^{-1}h \in H).$$

So $aH = bH (\Rightarrow\Leftarrow \because aH \neq bH)$.

⟧

এরপর দেখাব সাইজগুলো সমান--

Step 3: Each left coset has the same size as H:

Consider the function $f : H \to aH$ defined by $f(x) = ax$. Then

1. f is one-one:

   ⟦ Because:
   If $f(x_1) = f(x_2)$ then $ax_1 = ax_2$.
   $\therefore x_1 = x_2$, cencelling a.
   ⟧

2. f is onto.

   ⟦ Because:
   For any $y \in aH$ we have $y = ah = f(h)$ for some $h \in H$.
   ⟧

So $f(x)$ is a bijection from H to aH. This proves that $|H| = |aH|$.

ব্যস্, কাজ প্রায় শেষ--

Step 4: There are finitely many (say n) distinct left cosets, as G is finite. Call these $a_1H, ..., a_nH$. These are mutually exclusive and exhaustive by steps 1 and 2. So

$$|G| = \sum_{i=1}^{n} |a_iH| = \sum_{i=1}^{n} |H| = n|H|.$$

Hence the result.

■

Exercise 4: Prove that the order of a subgroup of a finite group divides the order of the group.[5] **(2005,2013)**
HINT:
এটাই তো Lagrange's theorem, যেটা আমরা আগের অংকেই প্রমাণ করলাম। ■

2.2 Equivalence ব্যবহার করে প্রমাণ

আমরা দেখেছি coset-গুলো (left বা right) কীভাবে G-এর মধ্যে পাঁউরুটির স্লাইসের মত সাজানো থাকে। Coset-গুলোর মধ্যে কোনো intersection থাকে না, এবং পুরো G-টাই coset-দের তলায় ঢাকা পড়ে যায়, অর্থাৎ coset-গুলো মিলে G-এর একটা partition তৈরী হয়। আমরা এই বইয়ের প্রথম অধ্যায়েই দেখেছি যে, partition-এর সঙ্গে equivalence relation-এর একটা ওতপ্রোত সম্পর্ক আছে। একটা equivalence relation দেওয়া থাকলেই তা থেকে একটা partition পাওয়া যায়, এবং একটা partition দেওয়া থাকলেই তার পিছনে একটা equivalence relation খুঁজে পাওয়া যায়।
আমরা এতক্ষণ Lagrange's theorem-কে দেখেছি coset-দের দৃষ্টিভঙ্গী থেকে। চাইলে আমরা পুরো জিনিসটাকে কেবলমাত্র equivalence relation আর partition ব্যবহার করেও করতে পারতাম, তাতে coset-এর নামও উল্লেখ করতে হত না। এবার আমরা সংক্ষেপে ধারণা দেব, সেটা কী করে করা যায়।
নীচের অংকে দেওয়া আছে equivalence relation-টা কীভাবে নিতে হবে।

Example 9: Let H be a subgroup of a group G. A relation ρ on the set G is defined by

$$\rho = \{(a, b) \in G \times G \mid a^{-1}b \in H\}.$$

Prove that ρ is an equivalence relation on G.[4] **(1999,2012)**
SOLUTION: প্রথমে ρ বলে যে relation-টা দিয়েছে সেটাকে একটা উদাহরণ দিয়ে বুঝে নিই। ধরো আমাদের group-টা নিলাম $G = (\mathbb{Z}, +)$. আর $H = 3\mathbb{Z}$ নিলাম, মানে $H = \{0, \pm3, \pm6, ...\}$. তাহলে $a^{-1}b \in H$ মানে হল $(-a)+b \in 3\mathbb{Z}$ অর্থাৎ $b - a$-কে 3 দিয়ে ভাগ যায়। ব্যাপারটা কয়েকটা উদাহরণ দিয়ে বোঝা যাক।

- যেমন ধরো বললাম $\mathbb{Z}$-এর কোন কোন element এখানে 0-র সঙ্গে ρ দ্বারা সম্পর্কিত, সেটা বার করো। মানে এমন কী কী $n \in \mathbb{Z}$ আছে যাতে $(0, n) \in \rho$ হয়। এর জন্য n-কে 3 দিয়ে ভাগ যেতে হবে। সুতরাং $n \in H$ হলেই $(0, n) \in \rho$ হবে।
- এবার H-এর বাইরে কিছু একটা element নিই, ধরো 1. তাহলে কোন কোন $n \in \mathbb{Z}$ এই 1-এর সঙ্গে সম্পর্কিত? উত্তর হল--যে সব n-এর জন্য $n - 1$-কে 3 দিয়ে ভাগ যায়, মানে যে সব n-কে 3 দিয়ে ভাগ করলে 1 ভাগশেষ থাকে। আশা করি চিনতে পেরেছ যে, একেই আমরা আগে $1 + H$ আকারে লিখেছিলাম।

আন্দাজ করা যাচ্ছে যে, ρ-এর equivalence class-গুলোই হল H-এর coset-রা।
এবার দেখাব যে ρ-টা সত্যি সত্যিই একটা equivalence relation হবে।

Reflexive:

For any $a \in G$ we have $a^{-1}a = e \in H$, as H is a subgroup.

So $(a, a) \in \rho$.

Symmetric:

For any $a, b \in G$ with $(a, b) \in \rho$ we have $a^{-1}b \in H$.

> So $b^{-1}a = (a^{-1}b)^{-1} \in H$, as H is a subgroup.
>
> Hence $(b, a) \in \rho$.
>
> <u>Transitive:</u>
>
> For any $a, b, c \in G$ with $(a, b), (b, c) \in \rho$ we have $a^{-1}b, b^{-1}c \in H$.
>
> So $a^{-1}c = (a^{-1}b)(b^{-1}c) \in H$, as H is a subgroup.
>
> Thus ρ is reflexive, symmetric and transitive. Hence ρ is an equivalence, as required.

■

যেই G-এর উপরে একটা equivalence relation পেলাম, অমনি G-টা বিভিন্ন equivalence class-এ ভেঙে গেল। আগের উদাহরণটা থেকে বুঝতে পারছি যে, এই equivalence-এর class-গুলোই হল আসলে coset-গুলো। কিন্তু আমরা তো এখানে coset-এর ধারণাটা ব্যবহার করব না, Lagrange's theorem-এ পৌঁছব খালি equivalence আর partition ব্যবহার করে। তার জন্য ধাপগুলো এইরকম--

1. প্রথমে দেখাব যে, প্রতিটা equivalence class-এর সাইজই H-এর সাইজের সমান।

2. আগের বার দেখাতে হয়েছিল যে, coset-গুলো হল mutually exclusive এবং exhaustive. এখানে আর সেই দায় নেই, কারণ equivalence class-গুলো মিলে যে একটা partition হয়, সে তো আমরা এই বইয়ের প্রথম অধ্যায় থেকেই জানি।

3. এর পর দেখাতে হবে যে, H-এর সাইজ m হলে প্রতিটা equivalence class-এর সাইজও হবে m. যদি n-খানা equivalence class থাকে, তবে G-এর মোট সাইজ হবে mn. সুতরাং H-এর সাইজ দিয়ে G-এর সাইজ ভাগ যাবে। ব্যস্‌, সেটাই তো Lagrange's theorem.

এই ধাপগুলো বিস্তারিতভাবে কষে দেব না। নীচের অংকগুলোতে তুমি নিজেই সেগুলো করবে।

Exercise 5: Let G be any group, and let H be any subgroup of G. Let ρ be the equivalence defined as

$$\rho = \{(a, b) \in G \ : \ a^{-1}b \in H\}.$$

Then prove that each equivalence class has the same cardinality as H.

HINT:

দুটো set-এর cardinality সমান দেখানোর অমোঘ অস্ত্র তো জানোই--ওদের মধ্যে একটা bijection বার করা। ধরো $g \in G$ কিছু একটা element নিলে। g-এর equivalence class-টাকে লেখা যাক $[g]$. তাহলে এই $f : [g] \to H$-টাকে লক্ষ কর--

$$f(x) = x^{-1}g.$$

ব্যস্‌, এর বেশী আর বলে দেব না। তোমাকে দেখাতে হবে যে--

1. এটা সত্যিই $[g]$ থেকে H-এ একটা function, মানে $x \in [g]$ হলে $f(x) \in H$ হতে বাধ্য,

2. এই f-টা একটা bijection.

তাহলেই অংকটা হয়ে যাবে। ■

Exercise 6: আচ্ছা, যদি আগের অংকটায় $f : [g] \to H$ এইভাবে নিতাম--

$$f(x) = g^{-1}x,$$

তবেও কি কাজ চলত? ■

2.2.1 Equivalence-টা এলো কোথা থেকে?

লক্ষ কর, equivalence ব্যবহার করে এগোলে কোথাও coset ব্যবহার না করেই Lagrange's theorem দিব্যি প্রমাণ হয়ে যাচ্ছে। অনুমান করতে পারছ যে, equivalence-টার সঙ্গে coset-দের কোথাও একটা সম্পর্ক আছে। আমরা $(\mathbb{Z}, +)$-এর উদাহরণ নিয়ে দেখেছি যে, equivalence class-গুলোই আসলে coset-গুলো। এমনটা কী সব সময়েই হবে? এর জন্য মনে করে দ্যাখো যে, একই coset-কে একাধিকভাবে লেখা যায়। যেমন এই অধ্যায়ের গোড়াতে $(\mathbb{Z}, +)$-এর যে উদাহরণটা নিয়েছিলাম, সেখানে দ্বিতীয় সারিটাকে $1 + H$-ও লেখা যেত, আবার $4 + H$-ও লেখা যেত। ঠিক কখন $aH = bH$ হবে? তার জন্য a, b-র মধ্যে যে সম্পর্ক প্রয়োজন সেটাকে লিখে ফেললেই equivalence-টা চলে আসে। নীচের অংকটা সেটা নিয়েই।

Example 10: Let G be a group and H be a subgroup of G. Let $a, b \in G$. The prove that $aH = bH$ if and only if $a^{-1}b \in H$.[3] **(2006)**

SOLUTION:

> G group, H subgroup.
> To show $aH = bH \iff a^{-1}b \in H$.
> $\underline{\implies}$:
> Given: $aH = bH$.
> $\because H$ is a subgroup, $\therefore e \in H$.
> $\therefore b = be \in bH = aH$.
> $\therefore b = ah$ for some $h \in H$.
> $\therefore a^{-1}b = h \in H$, as required.
> $\underline{\impliedby}$:
> Given: $a^{-1}b \in H$.

এবার দেখাব $aH = bH$. শুরু করব $aH \subseteq bH$ দেখিয়ে--

> Take any $x \in aH$.

আমাদের কাজ হল $x \in bH$ দেখানো, মানে ওই a-টাকে কোনোভাবে b বানাতে হবে। তার একটা কায়দা হতে পারে a-টাকে ডান দিকে থেকে $a^{-1}b$ দিয়ে গুণ করে দেওয়া।

> Let $h = a^{-1}b$. Then $h \in H$.
> Then $x = ah_1$ for some $h_1 \in H$.
> So $x = ahh^{-1}h_1 = bh^{-1}h_1$.

এইখানেই সেই কৌশলটা করলাম, a-র ডান দিকে থেকে $h = a^{-1}b$ দিয়ে গুণ করলাম, যাতে $ah = b$ এসে যায়। কিন্তু h-টা তো আমাদের আমদানি করা, তাই h^{-1} দিয়ে ভারসাম্য রক্ষা করতে হয়েছে।

Now $h^{-1}H_1 \in H$.
$\therefore x = bh^{-1}h_2 \in bH$.
So $aH \subseteq bH$.

অন্য দিকটাও একইভাবে-

Similarly, interchanging a and b, $bH \subseteq aH$.
Hence $aH = bH$, as required.

■

নীচের অংকটাও একই সুরের। আগের অংকে শিখলাম কখন $aH = bH$ হয়। এর পরের অংকটা বলছে কখন এর উল্টোটা হয়--$aH \cap bH = \phi$.

Example 11: H is a subgroup of a group G and $a, b \in G$. Prove that

$$aH \cap bH = \phi \iff b \notin aH.$$

[2] **(2011.7c)**
SOLUTION:

$\underline{\Longrightarrow}$: Given $aH \cap bH = \phi$.
$b = be \in bH$. But $aH \cap bH = \phi$. So $b \notin aH$, as required.
$\underline{\Longleftarrow}$: Given $b \notin aH$.
Let, if possible, $aH \cap bH \neq \phi$.
Can pick some $x \in aH \cap bH$.
Then $x = ah_1 = bh_2$ for some $h_1, h_2 \in H$.
So $b = ah_1h_2^{-1} \in aH (\Rightarrow\Leftarrow)$.

■

2.3 Applications

এবার Lagrange's theorem-এর কিছু সহজ প্রয়োগ দেখি। গত অধ্যায়ে বলেছিলাম যে, G যদি কোনো finite group হয় আর $g \in G$ হয়, তবে g-এর order দিয়ে $|G|$ (মানে G-এর সাইজ বা order) ভাগ যায়। নীচের অংকে এটাই দেখাতে বলেছে।

Example 12: Prove that the order of every element of a finite group is a divisor of the order the group.[3] **(2010.7b)**
SOLUTION:

Let G be a finite group. Let $g \in G$.
$\because G$ is finite,

> $\therefore o(g)$ must be finite, say n.

এর একটা ফলশ্রুতি আমরা জানি, যেটা এখানে কাজে লাগবে--

> $\therefore \forall k \in \mathbb{Z} \quad g^k = g^r$, where r is the remainder of k upon division by n.

এবার g-র power-গুলো দিয়ে একটা subgroup বানাব--

> Then $H = \{g^0, g, ..., g^{n-1}\} \subseteq G$ is a subgroup of G.

এটা সংক্ষেপে প্রমাণ করে নিই। আমরা আগেই শিখেছি কী করে সহজে subgroup দেখাতে হয়। সেই কায়দাটাই কাজে লাগাব।

> ⟦ <u>Because:</u>
>
> $\because g^0 \in H, \ \therefore H \neq \phi$.
> For any $g^i, g^j \in H$,
>
> $$g^i\left(g^j\right)^{-1} = g^{i-j} = g^r \in H,$$
>
> where $r \in \{0, ..., n-1\}$ is the remainder of $i - j$ upon division by n.
>
> ⟧

এই subgroup-টা নিয়ে আমরা পরেও অনেক আলোচনা করব।

> So, by Lagrange's theorem, $|H|$ divides $|G|$,
> Now $|H| = o(g)$.
> $\therefore o(g)$ divides $|G|$, as required.

■

Example 13: True or false: There exists a subgroup with 5 elements in a group of 8 elements.[2]

(2002)

SOLUTION:

> The result is false. By Lagrange's theorem, the size of a subgroup must divide the size of the group. But $5 \not| 8$.

■

2.3.1 Euler's theorem

Example 14: State Lagrange's theorem on finite groups. Hence show that if p is a prime and

a is a positive integer such that p is not a divisor of a then

$$a^{p-1} \equiv 1(\bmod\ p).$$

[1+4] **(2009)**

SOLUTION: প্রথম অংশটা তো করেইছি। এবার দ্বিতীয় অংশটা। এখানে বলে রাখি যে, এই দ্বিতীয় অংশটা একটা বিখ্যাত theorem যাকে বলে **Euler's theorem.** (Euler-এর উচ্চারণ হল অয়লার, ইউলার নয়!)

> Second part: We consider the set $G = \{1, ..., p-1\}$ with binary operation
>
> $$a \otimes b = \text{remainder of } ab \text{ upon division by } p.$$

প্রমাণের মূল ধারণাটা সংক্ষিপ্ত--আমরা প্রথমে দেখাব $(G, \otimes)$ হল একটা group, যার identity হল 1. এটার সাইজ তো দেখতেই পাচ্ছ $p-1$. সুতরাং যাই $a \in G$ নাও না, $o(a)|(p-1)$ হবে। অতএব

$$\underbrace{a \otimes \cdots \otimes a}_{p-1 \text{ times}} = 1$$

হবে। আর তার মানেই তো $a^{p-1} \equiv 1(\bmod\ p)$, যেটা দেখাতে দিয়েছে!

> Step I: Shall show that $(G, \otimes)$ is a group.
>
> Closure: Take any $a, b \in G$. Then $a \otimes b$ is the remainder of ab upon division by p, and hence must lie in $\{0, ..., p-1\}$.

এবার দেখাব যে, remainder-টা 0 হতে পারে না।

> Let, if possible, the remainder be 0.
>
> Then $ab \equiv 0(\bmod\ p)$,
>
> and so $p|ab$.
>
> But p is prime, and hence either $p|a$ or $p|b$.
>
> This is impossible since $1 \leq a, b \leq p-1 \quad (\Rightarrow\Leftarrow)$.
>
> Associative: This follows from associativity of ordinary multiplication.
>
> Identity: 1 is the identity of G.
>
> ⟦ Because:
>
> $\forall a \in G \quad 1 \otimes a = a \otimes 1$ remainder of $1 \times a = a$ upon division by p. But since $1 \leq a \leq p-1$, hence the remainder is a itself.
>
> ⟧

এবার inverse দেখাব। এখানে যুক্তিটা সামান্য জটিল।

Inverse: Shall show that

$\forall a \in G \quad \exists b \in G \quad a \otimes b = b \otimes a = 1.$

∀a Take any $a \in G$.

$\because p$ is prime and $1 \leq a \leq p-1$,

$\therefore gcd(a,p) = 1$.

So, by Euclid's algorithm, $\exists m, n \in \mathbb{Z} \quad am + pn = 1$.

আশা করি, এই জিনিসটা তুমি classical algebra শেখার সময়ে শিখেছ। ছোটোবেলায় যেভাবে লম্বা ভাগের মত করে HCF (গসাগু) বার করতে Euclid's algorithm হল সেটারই পোশাকী নাম।

So $am \equiv 1 (\mathrm{mod}\ p)$.

In particular, $p \not| \, m$.

কারণ, $p|m$ হলে তো am-ও p দিয়ে ভাগ যেত, ভাগশেষ তাহলে 1 হল কী করে?

∃b Choose $b \in G$ as the remainder of m upon division by p.

Then

$$\begin{aligned} ab &\equiv am (\mathrm{mod}\ p) \quad [\because b \equiv m (\mathrm{mod}\ p)] \\ &\equiv 1 (\mathrm{mod}\ p). \end{aligned}$$

$\therefore a \otimes b = b \otimes a = 1$, as required.

Thus G is a group.

বাকি কাজ সামান্যই--

Step 2: The order of G is $p-1$. So, by consequence of Lagrange's theorem, for each $a \in G$ we have $o(a)|(p-1)$.

Hence $a^{p-1} \equiv 1 (\mathrm{mod}\ p)$, as required.

■

2.4 Lagrange's theorem-এর converse

Lagrange's theorem বলে যে, H যদি G-এর subgroup হয় (যেখানে G একটা finite group), তবে $|H|$ অবশ্যই $|G|$-এর একটা factor (উৎপাদক) হবে। যেমন এক্ষুণি যে অংকটা করলাম সেখানে $|G| = 8$ ছিল, কিন্তু 5 মোটেই 8-এর একটা factor ছিল না। কিন্তু যদি 5-এর জায়গায় 4 দিত, তবে? সেক্ষেত্রে আমরা ফাঁপরে পড়তাম, কারণ তাহলে সরাসরি Lagrange's theorem খাটানো যেত না। কারণ $|G|$-এর যে কোনো একটা factor দিলেই যে ওই সাইজের একটা subgroup পাওয়া যাবে, এমন কথা Lagrange's theorem-এর কোথাও বলা নেই। বস্তুতঃ এমন subgroup সব সময়ে পাওয়া যায়ও না। এরকমই একটা উদাহরণ চেয়েছে নীচের অংকটায়।

Example 15: State Lagrange's theorem and establish that the converse of Lagrange's theorem



Fig 7

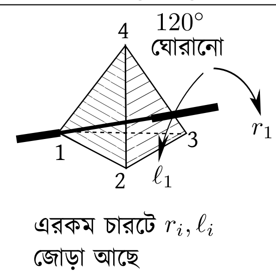


Fig 8

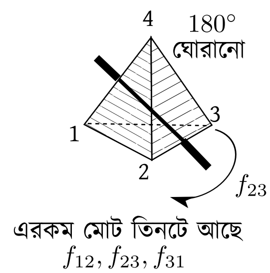


Fig 9

is not true.[2] **(2014)**

SOLUTION: Lagrange's theorem তো আগেই বলেছি। দ্বিতীয় অংশের ভাষাটা একটু গোলমেলে। "Establish" বলতে বোঝায় "প্রমাণ করা", কিন্তু সবচেয়ে ছোটো যে group-এর ক্ষেত্রে Lagrange's theorem-এর converse-টা খাটে না, তার সাইজই হল 12, এবং তার জন্য প্রমাণটাও মোটেই সংক্ষিপ্ত নয়। তাই অনুমান করছি যে, এখানে খালি counterexample-টুকু উল্লেখ করতে বলেছে, প্রমাণ চাইছে না।

> The group A_4 has size 12.
>
> 6 is a factor of 12.
>
> But A_4 has no subgroup of size 6.
>
> So the converse of Lagrange's theorem is false.

এই অতি সংক্ষিপ্ত উত্তরে যারা ধন্দে পড়ে গেছ তাদের সুবিধার্থে একটু বিশদ করি-- আমরা ত্রিভুজের উদাহরণে একটা সমবাহু ত্রিভুজকে নানা ভাবে ঘুরিয়ে ফ্রেমে ফিট্ করে বসাচ্ছিলাম। কাজটা 6-ভাবে করা যাচ্ছিল, যাদের নিয়ে একটা group হয়েছিল। যদি একই কাজ করতাম একটা regular tetrahedron-কে নিয়ে (Fig 7), তবে দেখা যেত যে কাজটা 12-ভাবে করা যায়, এদের নিয়ে যে group-টা হয়, সেটাই হল A_4. এদের মধ্যে এক জন তো e. বাকিদের মধ্যে আটজনের ছবি দেখিয়েছি Fig 8-এ, আর অবশিষ্ট তিন জনের ছবি রয়েছে Fig 9-এ। কেন A_4-এর মধ্যে কোনো 6 সাইজের subgroup নেই, সেটা বোঝা যায় এইভাবে-- খানিকটা (বে--শ খানিকটা) চিন্তা করলেই বুঝবে যে, যদি এরকম কোনো subgroup থাকে, তবে তার মধ্যে অন্ততঃ তিনটে r_i থাকতে বাধ্য। ব্যস্, অমনি ওদের তিনটে inverse (মানে ℓ_i) সেই subgroup-এ ঢুকে পড়বে। আর e তো থাকবেই। এতেই তো 7 জন হয়ে গেল! ■

অতএব দেখা যাচ্ছে যে Lagrange's theorem-এর converse-টা সব সময়ে খাটে না। অমনি পণ্ডিতেরা উঠে পড়ে লেগেছেন এটা জানতে যে, বাড়তি আর কী কী শর্ত চাপালে converse-টাও ঠিক হবে। এই গবেষণার ফলে জানা গেছে--

1. যদি group-টার সাইজ কোনো prime (মৌলিক) সংখ্যার power হয়, মানে p^n জাতীয় হয়, যেখানে p হল prime আর $n \in \mathbb{N}$, তবে converse-টা ঠিক হতে বাধ্য।

2. যদি group-টা Abelian হয়, তবেও converse-টা ঠিক হবে।

3. Group-টা যাই হোক না কেন, যদি তার সাইজের কোনো একটা prime factor নাও, তবে সেই সাইজের একটা subgroup থাকতে বাধ্য। একে বলে **Cauchy's theorem** (Cauchy-র উচ্চারণ হল কোশি, কচি নয়!)। যেমন $|G| = 12$ হলে 2 আর 3 হল এর দুটো prime factor. সুতরাং G-এর মধ্যে 2 সাইজের একটা আর 3 সাইজের একটা subgroup থাকবেই।

যাই হোক, এই সব গবেষণা এই বইয়ের এক্তিয়ারের বাইরে। নীচের অংকটা দেওয়া হয়েছে তোমাকে এই ব্যাপারটার একটা স্বাদ দেওয়ার জন্য। এই অংকটা Cauchy's theorem দিয়ে এক লাইনে করা যায় বটে, কিন্তু আমরা এখানে সরাসরি করব।

Example 16: If $(G, \circ)$ is a non-Abelian group of order 10, then prove that it must have a subgroup of order 5.[2] **(2012.1b)**

SOLUTION:

> By Lagrange's theorem, any non-identity element in G must have order 2 or 5 or 10.

এবার দেখাব যে, কারোর order-ই 10 হতে পারে না।

> Let, if possible, $\exists a \in G \quad o(a) = 10$.
> Then $G = \{a^0, a, a^2, ..., a^9\}$, and so G is Abelian($\Rightarrow\Leftarrow$).

কারণ $a^i \circ a^j = a^{i+j} = a^j \circ a^i$.

> So no element in G can have order 10.

এবার দেখাব সবগুলো non-identity element-এর order-ই 2 হতে পারে না।

> Let, if possible, all non-identity elements have order 2.
> Then $\forall a \in G \quad a^{-1} = a$. So
> $$\forall a, b \in G \quad a \circ b = (a \circ b)^{-1} = b^{-1} \circ a^{-1} = b \circ a,$$
> and hence G becomes Abelian($\Rightarrow\Leftarrow$).

তাহলে পড়ে রইল একটাই কেস--

> So $\exists a \in G \quad o(a) = 5$.
> Thus $\{a^0, a, a^2, a^3, a^4\}$ is a subgroup of size 5, as required.

■

DAY 3
Cyclic groups (part 1)

আমরা গতকালই দেখেছি যে, যদি কোনো group-এর element-এর order হয় k, তবে $\{g^0, g, ..., g^{k-1}\}$ একটা subgroup হয়, কারণ বাকি সব power-ই ঘুরেফিরে এই কয়টাতেই ফিরে আসে, যেহেতু $g^k = e$. এইভাবে অনেক সময়েই দেখা যায় যে একই কাজ বার বার করতে করতে আবার গোড়াতেই ফিরে আসা হয়। লুডো খেলায় যেমন তিন ছক্কা পড়লে কাটাকাটি হয়ে গিয়ে আবার নতুন করে হিসেব শুরু হয়। তারপর আবার ছক্কা পড়লে সেটাকে নতুন করে খালি এক ছক্কা ধরা হয়। আরেকটা উদাহরণ এইরকম-- ঘড়ির ঘন্টার কাঁটাটাকে যদি এক ঘর এক ঘর করে সরাতে থাকি, তবে বারো বার এরকম করার পর আবার প্রাথমিক অবস্থানেই ফিরে আসব। যেখানেই এমনটা হবে, সেখানেই জানবে একটা cyclic group আছে। ধরো "ঘন্টার কাঁটাটাকে একঘর ঘোরানো"-র নাম দিলাম r. তাহলে পরপর দুইবার r লাগানোর মানে কাঁটাটাকে দুই ঘর ঘোরানো, অর্থাৎ r^2 হল "দুই ঘর ঘোরানো"। আদৌ যদি না ঘোরাই, তবে সেটাকে লিখতে পারি r^0 হিসেবে। যদি উল্টোদিকে

একঘর ঘোরাই, তবে সেটা হবে r^{-1}. অর্থাৎ আমি যেদিকেই যতবার ঘোরাই না কেন, সেটাকে r-এর একটা power হিসেবে লেখা যাবে। কিন্তু যেহেতু বারো বার ঘোরালে আবার প্রাথমিক অবস্থানে ফিরে যাব, তাই আসলে r-এর বারোটা power-ই খালি আলাদা আলাদা--

$$r^0, r^1, r^2, ..., r^{11}.$$

বাকি সব power-ই এদের কারো না কারো সঙ্গে মিলে যাবে। যেমন $r^{12} = r^0$ বা $r^{-2} = r^{10}$. এই 12 জনের set-টা দিয়ে তৈরী হয় একটা **cyclic group.** এখানে binary operation-টা হচ্ছে এই রকম--

$$r^i r^j = r^{i \oplus j},$$

যেখানে $i \oplus j$ মানে $i + j$-কে 12 দিয়ে ভাগ করে remainder নেওয়া। যেমন $r^6 r^8 = r^{6\oplus 8} = r^2$, কারণ $6 + 8 = 14$-কে 12 দিয়ে ভাগ করলে remainder থাকে 2.

লক্ষ কর যে, দুটো power গুণ করার সময়ে আমরা exponent দুটোকে (অর্থাৎ ওপর তলার সংখ্যাদুটোকে) যোগ করছি modulo 12. তাই এক দিক দিয়ে দেখতে গেলে এই group-টা আসলে $(\mathbb{Z}_{12}, \oplus)$-এরই একটা অন্য রূপ। সেখানে বলতাম $6 \oplus 8 = 2$ আর এখানে বলছি $r^6 r^8 = r^2$.

শুধু আমাদের ঘন্টার কাঁটার group-টাই নয়, আসলে যেকোনো finite cyclic group-ই কোনো কোনো $(\mathbb{Z}_n, \oplus)$-এর রূপভেদ। যদি মিনিটের কাঁটা নিয়ে group বানাতাম তবে সেটা 60 ঘর সরলে তবে গোড়ার জায়গায় ফিরত। অর্থাৎ এক ঘর সরাকে যদি s লিখি তবে $s^{60} = s^0$ হত, আর group-টা হত

$$\{s^0, s^1, s^2, ..., s^{59}\}.$$

এটা বোঝা কঠিন নয় যে এই group-টা আসলে $(\mathbb{Z}_{60}, \oplus)$ ছাড়া আর কিছুই নয়।

এইধরণের group-কে cyclic group বলার কারণ এই যে, এদের সবার পিছনেই মূল কথা হল--কিছু একটা জিনিস চক্রাকারে ঘুরতে ঘুরতে এক সময়ে আবার প্রাথমিক অবস্থানে ফিরে আসছে। এই চক্র বা cycle থেকেই cyclic নামের উদ্ভব।

এই ব্যাখ্যার খালি একটা ব্যতিক্রম আছে। সেটা হল **infinite cyclic group.** এক্ষেত্রে যেন চক্রটার পরিধি infinite পরিমাণ লম্বা। Infinite cyclic group পৃথিবীতে একটাই আছে, এবং সেটা আমাদের পরমপ্রিয় অতিপরিচিত $(\mathbb{Z}, +)$. এটাকে cyclic group বলার কারণ এই যে যদি তুমি পর পর 1-এর সাথে 1 যোগ করে যেতে থাকো তবে যাবতীয় natural number-গুলো পাবে, কিন্তু কোনো দিনই এভাবে তুমি 0-তে ফিরতে পারবে না (যেমন ফেরা যেত $\mathbb{Z}_n$-এর বেলায়)। Negative number-গুলোকে পেতে ক্রমাগত 1 বিয়োগ করে যেতে হবে। তার মানে খালি 1 যোগ-বিয়োগ করেই গোটা $\mathbb{Z}$-টা বানানো সম্ভব। সেই কারণেই $\mathbb{Z}$-কে cyclic group বলে। এবার তবে নীচের অংকের উত্তরে cyclic group-এর সংজ্ঞাটা লিখে ফেলা যাক।

Example 17: Define a cyclic group.[1] **(2009,2007,2004,2000,1998)**

SOLUTION:

DEFINITION: Cyclic group

A group $(G, \star)$ called a cyclic group if

$$\exists g \in G \quad \forall a \in G \quad \exists n \in \mathbb{Z} \quad a = g^n,$$

where

$$g^n = \begin{cases} \underbrace{g \star \cdots \star g}_{n \text{ times}} & \text{if } n > 0 \\ \text{identity} & \text{if } n = 0 \\ \underbrace{g^{-1} \star \cdots \star g^{-1}}_{-n \text{ times}} & \text{if } n < 0 \end{cases}$$

Such a g is called a generator of G.

সহজ ভাষায় বললে, সব element-কেই কোনো একটা element-এর power হিসেবে লেখা যায়। ■

3.1 Cyclic group মাত্রেই Abelian

Example 18: Prove that every cyclic group is Abelian.[2] **(2000)**

SOLUTION:

Let G be a cyclic group. To show that G is Abelian, ie,

$\forall a, b \in G ab = ba.$

$\forall a, b$ Take any $a, b \in G$.

Since G is cyclic, it is generated by some $g \in G$.

So $a = g^i$ and $b = g^j$ for some $i, j \in \mathbb{Z}$.

Now

$$ab = g^i g^j = g^{i+j} = g^{j+i} = g^j g^i = ba,$$

as required.

■

কিন্তু তা বলে commutative group মাত্রেই কিন্তু cyclic নয়! সেটাই নীচের অংকটা--

Example 19: True or false: Any finite commutative group is a cyclic group.[2.5] **(1998)**

SOLUTION:

> The result is false.
> Counterexample : Klein's 4-group, which is the power set of $\{1,2\}$ with symmetric difference (Δ) as the binary operation.

এবার বলি কেন এটা cyclic নয়--

> Here ϕ is the identity.
> For any set A, we have $A\Delta A = \phi$.
> So no element has order 4, which is the order of the group. So the group cannot be cyclic.

■

Exercise 7: Correct or justify the statement: Klein's 4-group is non-abelian, cyclic group.[2+2] **(2011.8b)**
HINT:
Statement-টার দুটো অংশই ভুল। সেটা আগের অংকেই দেখালাম। Correct করার পর হবে--

> Klein's 4-group is an Abelian but not a cyclic group.

■

Exercise 8: True or false: Klein's 4-group K_4 is a cyclic group.[2] **(2006)**
HINT:
উত্তরটা যে false, সেটা তো এক্ষুণি দেখলেই। ■

3.2 Examples

এবার আমরা cyclic group-এর কিছু উদাহরণ দেখব।

3.2.1 $(\mathbb{Z}_n, \oplus)$

সবচেয়ে সহজ cyclic group হল $(\mathbb{Z}_n, \oplus)$. এর সঙ্গে আগেই পরিচয় হয়েছে। বস্তুতঃ যদি কোনো finite cyclic group থাকে যার সাইজ হল n, তবে তুমি সেটাকে সব সময়েই $(\mathbb{Z}_n, \oplus)$ বলে ভাবতে পারো, এইভাবে--একটা n সাইজের cyclic group মানেই $\{g^0, g^1, g^2, ..., g^{n-1}\}$ জাতীয় জিনিস, যেখানে g হল একটা generator. যদি প্রতিটা g^i-এর বদলে আমরা i কল্পনা করি, তবেই সেটা হয়ে যাবে $\{0, ..., n-1\}$ আর binary operation-টা হয়ে যাবে $\oplus$, মানে এমনি যোগের পরে n দিয়ে ভাগ করে ভাগশেষ নেওয়া।
$(\mathbb{Z}_n, \oplus)$-এর একটা generator হল 1.

Example 20: $(\mathbb{Z}_6, \oplus)$-এর মধ্যে 5 কি একটা generator? আর 3?

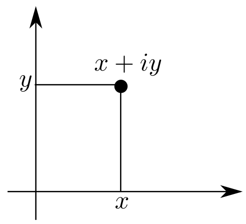


Fig 10

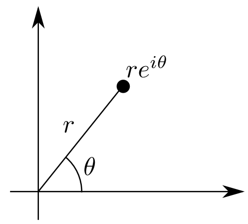


Fig 11

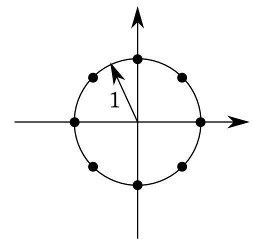


Fig 12

SOLUTION: 5-এর সঙ্গে 5 পর পর যোগ করতে থাকো, দ্যাখো $\mathbb{Z}_6$-এর সবগুলো element একে একে পাও কিনা--

$$\begin{aligned} 5 &= 5 \\ 5 \oplus 5 &= 4 \\ 5 \oplus 5 \oplus 5 &= 3 \\ 5 \oplus 5 \oplus 5 \oplus 5 &= 2 \\ 5 \oplus 5 \oplus 5 \oplus 5 \oplus 5 &= 1 \\ 5 \oplus 5 \oplus 5 \oplus 5 \oplus 5 \oplus 5 &= 0. \end{aligned}$$

এখানে $0, 1, ..., 5$ সবাইকেই পাওয়া গেল, তাই 5 একটা generator.
কিন্তু 3-এর বেলায় ব্যাপারটা এত দূর গড়াবে না--

$$\begin{aligned} 3 &= 3 \\ 3 \oplus 3 &= 0. \end{aligned}$$

ব্যস্, এরপর থেকে খালি 3 আর 0-র মধ্যেই আটকে থাকবে। সুতরাং 3 একটা generator নয়। ■

3.2.2 Complex

এবার আমরা complex number দিয়ে একটা অংক করব। তার জন্য হায়ার সেকণ্ডারী থেকে কটা জিনিস মনে করে নেওয়া যাক। Complex number-দের set-কে লেখে $\mathbb{C}$, যাকে একটা গ্রাফকাগজের মত ভাবা যায় (Fig 10)। কোনো complex number-কে $x + \mathbf{i}y$ আকারে ছাড়াও আরেকভাবে লেখা যায়, তাকে বলে polar form, $z = r\,e^{\mathbf{i}\theta}$ (Fig 11)। এই আকারে লিখলে কোনো complex number-এর power বার করতে সুবিধা হয়, যেমন $z^n = r^n\,e^{\mathbf{i}n\theta}$. আরেকটা ব্যাপার মনে করিয়ে দিই, যদি $r\,e^{\mathbf{i}\theta} = 1$ হয়, তবে $r = 1$ হবেই, এবং θ হবে $2k\pi$ আকারের।

Example 21: Let $S = \{z \in \mathbb{C} : z^n = 1\}$ where $\mathbb{C}$ is the set of all complex numbers. Show that S is a cyclic group w.r.t. to usual multiplication in $\mathbb{C}$. [4] **(2006)**

SOLUTION:

> We know that the $z^n = 1$ iff
>
> $$z = e^{\frac{2k\pi}{n}\mathbf{i}}, \quad k = 0, 1, ..., n-1.$$

এই জায়গাটা ভালো করে বুঝে নাও। যদি $z = r\,e^{\mathbf{i}\theta}$ নিই, তবে $z^n = 1$ মানে $r^n\,e^{\mathbf{i}n\theta} = 1$. তাই $r = 1$ আর $\theta = \frac{2k\pi}{n}$ হতে বাধ্য। ছবি দিয়ে ভাবলে S-এর element-গুলো সবাই complex plane-এ 1 radius-ওয়ালা circle-এর উপর সমান সমান অন্তরে সাজানো আছে। Fig 12-এ $n = 8$ কেসটা দেখিয়েছি।

If we take $a = e^{\frac{2\pi}{n}\mathbf{i}}$, then

$$S = \{a^0, a, a^2, ..., a^{n-1}\}.$$

Shall show that S is a group under complex multiplication.

Closure: $\because a^n = 1$,
$\therefore$ for any $a^i, a^j \in S$,

$$a^i a^j = a^{i+j} = a^r \in G,$$

where $r \in \{0, ..., n-1\}$ is the remainder of $i + j$ upon division by n.

Associativity: Inherited from $\mathbb{C}$.

Identity: We know that 1 is the identity for complex multiplication. Now $1 = a^0 \in S$. So 1 is the identity of S.

Inverse: For any $a^i \in S$ its inverse is $a^{n-i} \in S$, since $a^i a^{n-i} = a^{n-i} a^i = a^n = 1$.

So S is a group. Since all its elements can be expressed as powers of a, hence S is a cyclic group generated by a.

■

3.2.3 বিবিধ

Example 22: Let $G = \{2^n : n \in \mathbb{Z}\}$, where $\mathbb{Z}$ is the set of integers. Prove that G forms a cyclic group w.r.t. multiplication.[3] **(2002)**

SOLUTION:

Shall show that G is a group under multiplication.

Closure: Take any $2^m, 2^n \in G$. Then $2^m 2^n = 2^{m+n} \in G$.

Associative: Inherited from multiplication of $\mathbb{R}$.

Identity: 1 is the identity of multiplication in $\mathbb{R}$. Since $1 = 2^0 \in G$, hence 1 is the identity of G.

Inverse: Take any $x \in G$. Then $x = 2^n$ for some $n \in \mathbb{Z}$.
Then $x^{-1} = 2^{-n} \in G$ because $2^n 2^{-n} = 2^{-n} 2^n = 1$.
Thus G is a group.

By the definition, G, is made of integer powers of 2. Thus, G must be a cyclic grup generated by 2.

■

Example 23: Give an example of an infinite cyclic group.[1] **(2009.7ai)**

SOLUTION:

> $(\mathbb{Z}, +)$ is an example of an infinite cyclic group. It is generated by 1.

■

Example 24: True or false: The group $(\mathbb{Q}, +)$ of all rational numbers w.r.t. usual addition is a cyclic group.[2.5] **(1997,2001,2006)**

SOLUTION:

> The result is false.

কেন false সেটা আন্দাজ করা কঠিন নয়। যদি $(\mathbb{Q}, +)$ একটা cyclic group হত, তবে তার কিছু একটা generator থাকত q. সেক্ষেত্রে যেকোনো rational number-কেই q বা $\pm 2q$ বা $\pm 3q$ ইত্যাদি আকারে লেখা যেত। কিন্তু $q/2$-ও একটা rational number, তাকে তো কোনোভাবেই nq বা $-nq$ হিসেবে লেখা যায় না, কারণ $1/2$ একটা integer নয়।

> Let, if possible, $\mathbb{Q}$ be cyclic. Let $q \in \mathbb{Q}$ be a generator. Then
>
> $$\mathbb{Q} = \{nq : n \in \mathbb{Z}\}.$$
>
> Clearly, $q \neq 0$, since otherwise $\mathbb{Q} = \{0\}$.
>
> Now $q/2$ is a rational number, and so we must have
>
> $$\frac{q}{2} = nq$$
>
> for some $n \in \mathbb{Z}$. Since $q \neq 0$, this means $\frac{1}{2} = n \in \mathbb{Z} (\Rightarrow\Leftarrow)$.

■

Exercise 9: Is $(\mathbb{R}, +)$, the group of real numbers under addition, a cyclic group? **(1999)**

HINT:

আগের অংকের যুক্তি এখানেও প্রযোজ্য। ■

3.3 কখন cyclic হয়?

একটা finite group দেওয়া থাকলে cyclic কিনা সেটা বুঝব কীভাবে? দুটো হদিস দেওয়া আছে নীচের অংক দুটোতে।

Example 25: Prove that a group G of order n is cyclic if and only if there exists an element of order n in G.[3] **(2009,1998)**

SOLUTION:

> Let G be cyclic of order n. Then it is generated by some element $a \in G$.
> Thus,
> $$G = \{a^0, a, ..., a^{n-1}\}.$$
> Since $|G| = n$, this means $a^0, a, ..., a^{n-1}$ are all distinct.
> So $a^0 = e$ and $a, a^2, ..., a^{n-1} \neq e$.

এবার দেখাব যে, $a^n = e$, কারণ তাহলেই প্রমাণ হয়ে যাবে $o(a) = n$.

> Now $a^n \in G$. So $a^n = a^k$ for some $k \in \{0, 1, ..., n-1\}$.
> Thus $a^{n-k} = e$.
> Since $n - k \in \{1, ..., n\}$, and $a, a^2, ..., a^{n-1} \neq e$,
> hence $n - k = n$, ie, $k = 0$. So $a^n = a^0 = e$.
> This means $o(a) = n$, as required.

এবার উল্টো দিকটা--

> Conversely, if $b \in G$ has order n, then $b^0, b, ..., b^{n-1}$ are n distinct elements in G.
>
> [[Because:
>
> Let, if possible, $b^i = b^j$ for some $i < j \in \{0, ..., n-1\}$.
> Then $b^{j-i} = e (\Rightarrow\Leftarrow \because 0 < j - i \leq n-1)$.
>
>]]
>
> Since $|G| = n$, so we must have
> $$G = \{b^0, b, ..., b^{n-1}\},$$
> ie, G is cyclic, as required.

■

Exercise 10: Prove that a finite group $(G, *)$ of order n is cyclic iff there exists an element b in G such that $o(b) = n$. **(2014.1a)**
HINT: আগের অংকটাই। ■

Example 26: Prove that every group of prime order is cyclic.[3] **(2000,2007,2011,2012,2014)**

SOLUTION:

> Let G be a group of prime order p. Since $p \geq 2$, G has at least one element other than e. Let $a \in G$ such that $a \neq e$.
> We know that the order of an element must divide the order of the

> group. So $o(a)|p$. Since p is prime this means either $o(a) = 1$ or $o(a) = p$. But since $a \neq e$, so $o(a) \neq 1$. Hence we must have $o(a) = p$.

এবার ব্যাপারটা কিন্তু আগের অংকটার মতই হয়ে গেল। আগের অংকটা একটা standard result, তাই সেটাকে সরাসরি ব্যবহার করে দেব।

> Thus, $a^0, a, ..., a^{p-1}$ are p distinct elements in G. Since $|G| = p$, we must have
> $$G = \{a^0, a, ..., a^{p-1}\},$$
> ie, G is generated by a. So G is cyclic.

■

একটা ছোট্টো প্রয়োগ দেখি।

Example 27: True or false: Every group of order less than 4 is commutative.[2] **(2005)**

SOLUTION:

> The statement is true. If a group G is of size 1, then G contains only the identity element, and hence is commutative.
>
> If G has size 2 or 3, which are prime, then by standard result, G must be cyclic, and hence commutative.

এই "standard result"-টা হল আগের অংকটাই।
এই প্রসঙ্গে বলে রাখা ভালো যে 4 বা 5 সাইজের group-রাও কিন্তু সব সময়ে commutative হয়। দুনিয়ায় সবচেয়ে ছোটো non-commutative group-এর সাইজ হল 6. সেই group-টার সঙ্গে আমাদের ইতিমধ্যেই মোলাকাত হয়েছে, কারণ সেটাই হল সেই ত্রিভুজের উদাহরণের group-টা। ■

DAY 4
Cyclic groups (part 2)

4.1 Generators

আমরা গতকাল দেখেছিলাম যে, $(\mathbb{Z}_6, \oplus)$-এর মধ্যে 5 একটা generator, কিন্তু 3 নয়। তার কারণ 5-এর সঙ্গে 5 বার বার যোগ করে গেলে 6 বারের আগে 0 আসত না। কিন্তু 3-এর সঙ্গে 3 যোগ করতেই 0 হয়ে যাচ্ছিল। একইরকম কারণে 4-ও একটা generator হবে না, কারণ $4 \oplus 4 \oplus 4 = 0$ হয়ে যাবে। একটু চিন্তা করলেই বুঝবে যে, generator হবার জন্য এমন কোনো k দরকার যাতে $k, 2k, 3k, ..., 5k$ এরা কেউই 6 দিয়ে ভাগ না যায়। মানে 6-এর সাথে k-র কোনো common factor থাকলে চলবে না। একই কথা খাটে যে কোনো finite cyclic group-এর ক্ষেত্রেই--

THEOREM

Let G be a cyclic group of order n. Let g be a generator. Then g^i is a generator iff $gcd(n, i) = 1$.

প্রমাণের মূল ধারণাটা এরকম--ধরো g^i-কে নাম দিলাম a. তবে a-টা কখন একটা generator হবে? যখন, $a^0, a, a^2, ..., a^{n-1}$ এরা সবাই আলাদা আলাদা হবে। তার মানে $a, a^2, ..., a^{n-1}$-রা কেউ identity-র সমান হয়ে যাবে না। (যেমন $a^2 \neq a^5$ হওয়া মানে $a^3 \neq e$)। অর্থাৎ যাই $k \in \{1, ..., n-1\}$ নাও না কেন, $a^k = (g^i)^k = g^{ik} \neq e$. যেহেতু $o(g) = n$, তাই এর মানে হল $\forall k \in \{1, ..., n-1\} \quad n \nmid ik$. এবং সেটা হবে তখনই যখন $gcd(n, i) = 1$ হবে, কারণ n আর i-এর যদি কোনো common factor থাকে যেটা > 1, তবে ik-এর মধ্যেও সেই factor-টা আছে। সুতরাং ওতেই n-এর খানিকটা কেটে গেল। এরপরে n-এর যেটুকু বাকি রইল সেটাকে k নিলেই $n|ik$ হয়ে যেত।

Example 28: Suppose that G is a cyclic group of order 7 and a is a generator of it. Determine all generators of G.[2] **(2009.8bi)**

SOLUTION:

> We know that, for $i = 0, 1, ..., 6,\ a^i$ is a generator iff $gcd(i, 7) = 1$.
>
> Since 7 is a prime number, hence $gcd(i, 7) = 1$ iff $i = 1, ..., 6$.
>
> So $a, a^2, ..., a^6$ are all the generators of G.

■

Example 29: Let $S = \{z \in \mathbb{C} : z^n = 1\}$ where $\mathbb{C}$ is the set of all complex numbers. Show that S is a cyclic group w.r.t. to usual multiplication in $\mathbb{C}$. Find all possible generators of the group.[5] **(2006)**

SOLUTION: প্রথম অংশটা আমরা গতকালই করেছি Example 21-এ। এবার দ্বিতীয় অংশটা করব।

> Second part: Here $a = e^{\frac{2\pi}{15}\mathbf{i}}$ is a generator.
>
> We know that $a^k \in G$ generates $G \iff gcd(k, 15) = 1$.
>
> So the set of all possible generators of the group is
>
> $$\{e^{\frac{2k\pi}{15}\mathbf{i}} : k = 1, 2, 4, 7, 8, 11, 13, 14\}.$$

■

Example 30: If g is a generator of a cyclic group, show that g^{-1} is also a generator of it. What are the generators of $(\mathbb{Z}, +)$?[3+1] **(2004)**

SOLUTION:

<u>First part</u> : Let G be a cyclic group with generator g. Shall show g^{-1} is also a generator of G.

Since g generates G,

$$G = \{g^n : n \in \mathbb{Z}\} = \{(g^{-1})^{-n} : n \in \mathbb{Z}\} = \{(g^{-1})^m : m \in \mathbb{Z}\},$$

writing $m = -n$ and using the fact $-\mathbb{Z} = \mathbb{Z}$.

এখানে $-\mathbb{Z} = \mathbb{Z}$ মানে--যাবতীয় integer-দের negative-এর set ফের $\mathbb{Z}$-ই হয়।

Hence G is generated by g^{-1}, as required.

<u>Second part</u> : $\mathbb{Z}$ has only two generators 1 and -1.

■

Example 31: True or false: An infinite cyclic group has only two generators.[2.5] **(1997)**

SOLUTION:

The result is true.

Let a be one generator (exists, since the group is cyclic).

Then a^{-1} is also another generator.

Clearly, $a \neq a^{-1}$, because otherwise $a^2 = e$, where $e =$ identity. and so a cannot generate an infinite group.

এবার দেখাতে হবে যে, এদের দুজন ছাড়া অন্য কোনো generator সম্ভব নয়।

Let b be any generator of G. Shall show that either $b = a$ or $b = a^{-1}$.

Since both a, b are generators, so $a = b^m$ and $b = a^n$ for some $m, n \in \mathbb{Z}$.

Thus $a = b^m = a^{mn}$. So $a^{mn-1} = e$.

Since a is of infinite order, this means $mn = 1$. So either $n = 1$ or $n = -1$.

কারণ দুটো integer-এর গুণফল 1 হওয়া একমাত্র তখনই সম্ভব যখন দুজনেই 1 বা -1.

So either $b = a$ or $b = a^{-1}$, as required.

■

Example 32: Prove that an infinite cyclic group has exactly two generators.[3] **(2010,2013)**

SOLUTION: আগের অংকটাই। ■

Example 33: Let $G = \{2^n : n \in \mathbb{Z}\}$, where $\mathbb{Z}$ is the set of integers. Prove that G forms a cyclic group w.r.t. multiplication. Find two generators of this group.[5] **(2002)**
SOLUTION: প্রথম অংশটা আগেই করেছি Example 22-এ। লক্ষ কর যে, G-টা আসলে ছদ্মবেশে $(\mathbb{Z}, +)$ কারণ $2^m \times 2^n = 2^{m+n}$, সুতরাং power-এর উপর তলার integer-দুটো যোগ হচ্ছে। $\mathbb{Z}$-এর বেলায় generator জানি 1 আর -1. সুতরাং এখানে--

> Two generators are 2 and 2^{-1}.

■

Example 34: True or false: If a, b are two distinct generators of a cyclic group G, then ab is also a generator.[2] **(2003,2005)**
SOLUTION:

> The result is false. $a = 1$ and $b = -1$ are both generators of $G = (\mathbb{Z}, +)$.
> But $ab = 1 + (-1) = 0$ is not a generator of $\mathbb{Z}$,

এখানে মনে রেখো যে, ab মানে a আর b-কে group-এর binary operation-টা দিয়ে মেলানো। এখানে যেহেতু binary operation-টা হল $+$, তাই ab মানে এখানে আসলে $a + b$.
0 যে $\mathbb{Z}$-এর generator নয়, সেটা প্রায় বলাই বাহুল্য। তাও একটু কারণটা লিখেই দিই--

> because 0 has order 1, while $\mathbb{Z}$ is an infinite set.

■

4.2 Subgroup

এবার আমরা cyclic group-দের subgroup-দের নিয়ে মাথা ঘামাব। আমরা এখানে দুটো জিনিস শিখব--এক, cyclic-দের subgroup-রাও cyclic-ই হয়, আর দুই, cyclic group-দের ক্ষেত্রে Lagrange's theorem-এর converse-টাও ঠিক হয়।

4.2.1 Cyclic-দের subgroup-রাও cyclic

Example 35: Prove that every subgroup of a cyclic group is cyclic.[4] **(1999,2002,2006,2010)**

SOLUTION:

> Let $G = \{a^i \ : \ i \in \mathbb{Z}\}$ be a cyclic subgroup (finite/infinite) generated by some a. Let H be any subgroup of G. Shall show that H is cyclic.
> Let $S = \{i > 0 : a^i \in H\}$.
> <u>Case 1: $S = \phi$.</u> Here H is the trivial group, and hence cyclic.

Case 2: $S \neq \phi$.

Let k be the minimum element of S.

Let $b = a^k$.

দেখাব যে, H-টা এই b দিয়ে generated, মানে H-এর সব সদস্যই b-এর কোনো না কোনো power. তাতেই প্রমাণ হয়ে যাবে যে, H হল cyclic.

Take $h \in H$. Then $h = a^i$ for some $i \in \mathbb{Z}$.

আমাদের উদ্দেশ্য হল এটা দেখানো যে k দিয়ে i-কে ভাগ যায়।

Let q be the quotient and r be the remainder of i upon division by k. Thus,

$$i = qk + r \text{ where } 0 \leq r \leq k - 1.$$

দেখাব যে $r = 0$.

Then $h = a^{qk+r} = (a^k)^q a^r = b^q a^r$, or $a^r = b^{-q} h$.

Since $h, b \in H$ this means $a^r \in H$. But a^k is the smallest positive power of a in H. So $r \leq k - 1$ cannot be positive. So $r = 0$. and hence $h = b^q$.

Since $h \in H$ was arbitrary, this means each element of H is a power of b.

Thus, H is a generated by b, and hence is cyclic.

■

নীচের অংকটায় proper subgroup বলে একটা কথা ব্যবহার করা হয়েছে। এর মানে এমন একটা subgroup যেটা পুরো group-টার সমান নয়, "H is a proper subgroup of G" মানে "H হচ্ছে G-এর একটা subgroup এবং $H \neq G$.

Example 36: If $G = \{x : x^{15} = 1\}$ then show that all the proper subgroups of $(G, \bullet)$ are cyclic, where $\bullet$ denotes complex multiplication.[2] **(2004)**

SOLUTION:

We know that there are exactly 15 distinct roots of 1 in $\mathbb{C}$. These are

$$e^{\frac{2k\pi}{15}\mathbf{i}}, \quad k = 0, 1, ..., 14.$$

So this group is generated by a single element $a = e^{\frac{2\pi}{15}\mathbf{i}}$, and hence is cyclic.

We know that all subgroups of a cyclic group are cyclic. Hence all (proper) subgroups of G are cyclic, as required.

■

একটা cyclic group-র সব subgroup-ই যে cyclic হয় সেটা আমরা দেখলাম। প্রশ্ন উঠতে পারে--এর উল্টো দিকটাও কী ঠিক? অর্থাৎ, যদি এমন একটা group থাকে যার প্রতিটা subgroup-ই cyclic তবে কী group-টাও cyclic হতে বাধ্য? এই প্রশ্নের উত্তর যে "হ্যাঁ", তা বলাই বাহুল্য, কারণ group-টা তো নিজেই নিজের একটা subgroup, তাই "সব subgroup-ই cyclic " বলার মধ্যে এটাও বলা হয়ে গেছে যে, group-টা নিজেই cyclic. কিন্তু যদি খালি বলে দিতাম যে, "সব proper subgroup-গুলো cyclic ", তবে? সেক্ষেত্রে উত্তর হত "না"। সেই নিয়েই এবারের অংকটা।

Example 37: Give an example of a finite group which is not cyclic, but whose all proper subgroups are cyclic. Justify your answer.[2] **(2003,2005)**

SOLUTION:

> We consider Klein's 4-group, $(\mathscr{P}(\{1,2\}), \Delta)$, where $\mathscr{P}(\{1,2\})$ is the power set of $\{1,2\}$, and Δ is the symmetric difference operation.
> Here ϕ is the identity.
> For any set A, we have $A\Delta A = \phi$.
> So no element has order 4, which is the order of the group. So the group is not cyclic.
> By Lagrange's theorem, the proper subgroups can only have sizes dividing 4 and < 4.
> So the sizes must be 1 or 2.
> A subgroup of size 1 is a trivial subgroup, and hence cyclic.
> Also a subgroup of size 2 must be cyclic (since 2 is a prime).

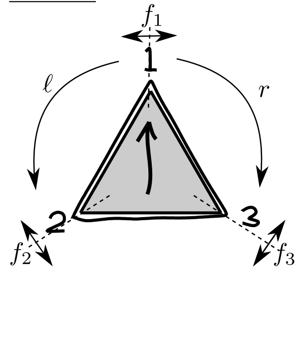
■

4.2.2 Cyclic-এর বেলায় Lagrange's theorem-এর converse

Cyclic group-দের বেলায় Lagrange's theorem-দের converse-টা সবসময়ে সত্যি। অর্থাৎ যদি G একটা cyclic group হয় যার সাইজ n, আর কোনো $d > 0$ দিয়ে n-কে ভাগ যায়, তবে d সাইজের একটা subgroup অবশ্যই G-এর মধ্যে থাকবে। শুধু তাই নয়, ওই সাইজের ঠিক একটাই subgroup থাকবে। এটাই প্রমাণ করতে বলেছে এবার।

Example 38: Let $(G, *)$ b a finite cyclic group of order n. Then prove that for every positive divisor d of n there exists a unique subgroup of G of order d.[3] **(2013.2a)**

Fig 13



SOLUTION:

> Existence : Let $G=\{a^0,a,...,a^{n-1}\}$.
> We have $n=dk$ for some k.
> Let $b=a^k$.
> Then $o(b)=d$, and hence $\{b^0,b,...,b^{d-1}\}$ is a cycic subgroup of order d in G, as required.
> Uniqueness : Let H be any subgroup of order d in G.
> Since any subgroup of a cyclic group must be cyclic, hece H must be cyclic.
> Let h be any generator of H.
> Then $h=a^i$ for some $i=0,...,n-1$.

■

DAY 5
Permutation groups (part 1)

আজকে আমরা একটা ভীষণ গুরুত্বপূর্ণ জিনিস শিখব। ব্যাপারটা বোঝার জন্য সেই ত্রিভুজের উদাহরণটা দিয়ে শুরু করি, যেখানে আমরা একটা ত্রিভুজাকার কাগজের টুকরোকে নানাভাবে একটা একই মাপের ফ্রেমে ফিট্ করে বসানোর চেষ্টা করছিলাম (Fig 13) কাজটা করা যেত ঠিক 6 ভাবে, যাদের নাম দিয়েছিলাম

$$e,r,\ell,f_1,f_2,f_3.$$

আমরা আগেই বলেছি যে এগুলো আসলে $\{1,2,3\}$ থেকে $\{1,2,3\}$-তে এককেটা function. যেমন

$$r(1)=3,\ \ r(2)=1,\quad r(3)=2. \qquad (*)$$

যেমন $r(1)=3$-এর অর্থ হল--ফ্রেমের 1 নম্বরে ত্রিভুজের যে প্রান্তটা ছিল, সেটা r লাগানোর ফলে যাবে ফ্রেমের 3 নম্বরে। এই function-গুলো নিয়ে আমরা binary operation করছিলাম function composition. যেমন $r\circ f_1$ বা $f_1\circ f_2$, এইরকম। যেভাবে (*)-এ লিখেছি সেভাবে লিখলে composition -গুলো মনে মনে বার করা কঠিন। সেই জন্য লোকে একটা সহজ notation ভেবেছে, যাকে আমরা বলব **double decker notation.**

5.1 Double-decker notation

কায়দাটা আর কিছুই নয় x যদি y-তে যায়, তবে x-এর নীচে y লিখব। যেমন r-এর বেলায় $1,2,3$ যায় যথাক্রমে $3,1,2$-তে। তাই লিখব

$$r=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}.$$

এখানে দুটো row রয়েছে। দুটো row-তেই $1,2,3$ লেখা। উপরের row-এর সংখ্যাগুলো হল শুরুর অবস্থান, আর নীচের row-টা হল কোথায় যাচ্ছে। এই পুরো জিনিসটাকে বলে একটা **permutation.** যার আক্ষরিক অর্থ হল পুনর্বিন্যাস। এখানে যেন উপরতলার $1,2,3$-গুলো ছিল তিনটে জিনিস, তাদের পুনর্বিন্যাস করে নীচের তলার $3,1,2$ পাওয়া গেল। নীচের অংকটা করে এই notation-টার সঙ্গে সড়গড় হয়ে নাও।

Exercise 11: নীচের প্রত্যেকটা ক্ষেত্রে কিছু একটা ভুল আছে। ভুলগুলো ধরতে পারো?

1. $\binom{1\ \ 2\ \ 2}{3\ \ 2\ \ 1}$
2. $\binom{1\ \ 4\ \ 2}{4\ \ 2\ \ 1}$
3. $\binom{1\ \ 2\ \ 3}{1\ \ 2\ \ 1}$

■

এই notation-টার অন্যতম সুবিধা এই যে, এটা ব্যবহার করে permutation-দের inverse এবং composition চট্ করে বার করে দেওয়া যায়। যেমন, যদি একটা permutation দেওয়া থাকে, তবে তুমি এইভাবে ধাঁ করে তার inverse-টা লিখে ফেলতে পারো--খালি উপরতলাকে নীচে এবং নীচের তলাকে উপরে নিয়ে গিয়ে। যেমন $r = \binom{1\ 2\ 3}{3\ 1\ 2}$-এর inverse হবে $r^{-1} = \binom{3\ 1\ 2}{1\ 2\ 3}$, বা যেটাকে সুন্দর করে লিখলে (মানে উপর তলার সংখ্যাগুলোকে ছোটো থেকে বড় সাজিয়ে লিখলে) হয়

$$r^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix},$$

যেটা আসলে ℓ. লক্ষ কর, উপরের তলার সংখ্যাগুলোকে সাজানোর সময়ে নীচের তলার সংখ্যাগুলোকেও তাল মিলিয়ে আগেপরে করতে হয়েছে। Double decker notation-এ এটাই নিয়ম--উপরের তলার সংখ্যাগুলোকে ছোটো থেকে বড় সাজিয়ে লেখা হয়।
দুটো permutation-এর composition-ও এই দোতলা notation থেকে সহজে বার করা যায়। যেমন ধরো

$$r = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \text{ এবং } f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

হলে $r \circ f_1$ বার করা যাবে এইভাবে--

$$\begin{array}{c|ccc} & 1 & 2 & 3 \\ f_1 & & & \\ & 1 & 3 & 2 \\ r & & & \\ & 3 & 2 & 1 \end{array}$$

এখানে একেবারে উপরের লাইন দুটোয় লিখেছি f_1, কারণ $r \circ f_1$ মানে আগে f_1 পরে r. সবার নীচের লাইনটা এসেছে r-এর দ্বিতীয় লাইন থেকে,
এবার প্রথম আর শেষের লাইনটুকু দেখলেই বুঝবে--

$$r \circ f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

নীচের কয়েকটা অংক করে হাত পাকিয়ে নাও।

Example 39: For the permutations

$$A = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix} \text{ and } B = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 4 & 5 & 2 \end{pmatrix}$$

find AB.[1] **(2002)**
SOLUTION:

$$\begin{array}{c|ccccc} & 1 & 2 & 3 & 4 & 5 \\ B & & & & & \\ & 1 & 3 & 4 & 5 & 2 \\ A & & & & & \\ & 2 & 1 & 5 & 4 & 3 \end{array}$$

So

$$AB = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 4 & 3 \end{pmatrix}.$$

■

Exercise 12: Find A^2, A^{-1} for the permutation

$$A = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}.$$

[1+2] **(2000)**

HINT:

এটা একেবারেই আগের অংকটার মত। নিজে নিজে করার চেষ্টা কর। ■

5.2 Cycle notation

Double-decker notation-টা বেশ কাজের জিনিস বটে, কিন্তু ওতে অনেকটা লিখতে হয়। এবার আমরা আরেকটা notation শিখব, যেটা অনেক সংক্ষেপে কাজ সারে। একে বলে **cycle notation.** একটা উদাহরণ নিয়ে বোঝা যাক।

তুমি যখন যাবে উলুবেড়ে তাঁর সঙ্গে দেখা করতে, তখন তিনি থাকবেন মতিহারি। যদি মতিহারি যাও, তাহলে শুনবে তিনি আছেন রামকিষ্টপুর, আবার সেখানে গেলে দেখবে তিনি গেছেন কাশিমবাজার।

--হ য ব র ল

Example 40: ধরো আমরা এই permutation-টাকে cycle notation-এ লিখতে চাই--

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 9 & 7 & 2 & 4 & 6 & 1 & 5 & 8 \end{pmatrix}.$$

কী করে করব?

SOLUTION:

- প্রথমে 1 কোথায় যাচ্ছে দেখি। 1 যাচ্ছে 3-এ। সুতরাং একটা cycle শুরু হচ্ছে এইভাবে $(1, 3, \ldots)$. এবার দেখি 3 কোথায় গেছে, উত্তর হল 7-এ। সুতরাং cycle-টা আরেক ঘর এগোল--$(1, 3, 7\ldots)$. এবার খুঁজে দ্যাখো 7 আবার কোথায় গেছে। 7 গিয়ে বসে আছে 1 নম্বরে। আমরা তো 1 নিয়েই শুরু করেছিলাম। সুতরাং cycle-টা শেষ হল--$(1, 3, 7)$.
- এ বার এই cycle-এর বাইরে কিছু একটা নাও, ধরো 2. দ্যাখো 2 কোথায় গেছে। 9 নম্বরে। 9 আবার গেছে 8 নম্বরে। 8 গেছে 5 নম্বরে, 5 গেছে 4 নম্বরে, 4 ফিরে গেছে 2 নম্বরে। সুতরাং একটা লম্বা cycle পেলাম $(2, 9, 8, 5, 4)$.
- এবার দেখি এই দুটো cycle-এর বাইরে কেউ রয়ে গেল কিনা। এক্ষেত্রে 6 এখনো হিসেবে আসে নি। সুতরাং 6 নিয়ে শুরু করি। 6 কোথায় গেছে? কোথাও যায় নি, 6 নম্বর স্থানেই আছে। সুতরাং ওর জন্য cycle-টা হবে (6).।

সব মিলিয়ে আমরা পেলাম

$$\pi = (1,3,7)(2,9,8,5,4)(6).$$

এর মধ্যে যে সব cycle-এর দৈর্ঘ্য 1, (যেমন আমাদের ক্ষেত্রে (6)-এর দৈর্ঘ্য হচ্ছে 1), তাদেরকে লোকে আর আলাদা করে লেখে না। তাই আমরা লিখব--

$$\pi = (1,3,7)(2,9,8,5,4).$$

■

এক্ষুণি যেভাবে এগোলাম, সেটা যে কোনো permutation-এর ক্ষেত্রেই করা যায়। এইভাবে এগোলে একটা permutation-কে কিছু cycle-এর product হিসেবে লেখা যায়। এই প্রসঙ্গে তিনটে জিনিস লক্ষণীয়--

1. এর ফলে যে cycle-গুলো পাওয়া যায় তারা disjoint হতে বাধ্য, মানে একই সংখ্যা কখনও একাধিক cycle-এ থাকতে পারে না, কারণ প্রতিটা cycle শুরু করছি এমন সংখ্যা নিয়ে, যেটা আগের cycle-গুলোতে আসে নি। যে সব সংখ্যা যথাস্থানেই থাকে তাদের জন্য cycle-গুলোর দৈর্ঘ্য 1 হয়, সেগুলোকে আর আলাদা করে লেখা হয় না। সুতরাং একটা মাত্র permutation-কেই এভাবে cycle notation-এ লেখা যায় না, সেটা হল identity permutation, কারণ এখানে সব সংখ্যাই যথাস্থানে থাকে।

2. এখানে আমরা প্রথমে 1 থেকে খোঁজা শুরু করে $(1,3,7)$ পেয়েছিলাম, তারপর 2 থেকে শুরু করে পেয়েছিলাম $(2,9,8,5,4)$. যদি আমরা প্রথমে 2 থেকে খোঁজা শুরু করতাম, তবে $(2,9,8,5,4)$-কে আগে পেতাম। সেই কারণে আমরা π-কে এইভাবেও লিখতে পারি--

$$\pi = (2,9,8,5,4)(1,3,7).$$

   সুতরাং বুঝতেই পারছ যে, disjoint cycle-দের লেখার সময়ে কোন cycle-টা আগে লিখেছি আর কোনটা পরে, সেটা গুরুত্বপূর্ণ নয়।

3. $(1,3,7)$ বলে যে cycle-টা পেয়েছিলাম, সেটা আমরা 1 থেকে শুরু করেছিলাম। যদি 7 থেকে শুরু করতাম তবে $(1,3,7)$-এর বদলে পেতাম $(7,1,3)$. বলাই বাহুল্য যে, $(1,3,7)$ আর $(7,1,3)$ আসলে একই cycle-কে দুভাবে লেখা। এটাকে চাইলে আমরা $(3,7,1)$ হিসেবেও লিখতে পারতাম। কিন্তু $(3,1,7)$ লিখে সেটা অন্য cycle বোঝাত।

সব মিলিয়ে বলতে পারি যে, identity ছাড়া যে কোনো permutation-কেই ঠিক একভাবেই disjoint cycle-এর product হিসেবে লেখা যায়। এখানে "একভাবেই" কথাটা বুঝে নাও-- কটা cycle এবং প্রতিটা cycle কার পরে কী কী সংখ্যা দিয়ে তৈরী সেটা unique. কিন্তু cycle-গুলোকে কোথা থেকে শুরু করে লিখছি সেটা নিয়ে মাথা ঘামাচ্ছি না, এবং কোন্ cycle-টা আগে আর কোন্ cycle-টা পরে লিখছি সেটা নিয়েও মাথা ঘামাচ্ছি না।

Exercise 13: If $\alpha = (1\ 3\ 4)(5\ 6)(2\ 7\ 8\ 9)$ and

$$\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 8 & 9 & 6 & 4 & 5 & 2 & 3 & 1 \end{pmatrix}$$

Fig 14

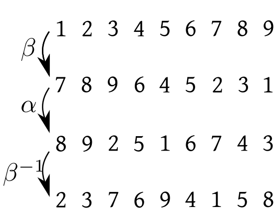


Fig 15

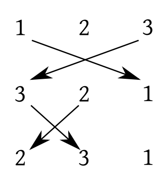


Fig 16

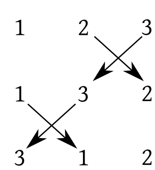
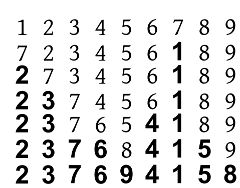


Fig 17



are two permutations, find the product $\gamma = \beta^{-1}\alpha\beta$. Justify whether γ can be expressed as the product of transpositions uniquely? **(2012.2)**

HINT:

প্রথম অংশটা তো তোমার অনায়াসেই করতে পারা উচিত। করলে দেখবে উত্তর আসছে

$$\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 3 & 7 & 6 & 9 & 4 & 1 & 5 & 8 \end{pmatrix}$$

যদি বুঝতে না পারো, তবে Fig 14 দেখে নাও। পরের অংশে product of transposition হিসেবে ভেঙে লেখার কথা রয়েছে। এখানে transposition মানে হল দুটো সংখ্যার স্থানবিনিময়। Cycle দিয়ে ভাবলে transposition হল 2 দৈর্ঘ্যের একটা cycle, যেমন 3 আর 5 স্থানবিনিময় করলে সেটা হবে $(3,5)$ (বা $(5,3)$)। আর "product" বলতে এখানে বোঝাচ্ছে একটার পর একটা করা। এটা আসলে function composition ছাড়া আর কিছুই নয়। যেমন, যদি $\{1,2,3\}$ নিয়ে কাজ করি, তবে $(2,3)(1,3)$ মানে হল প্রথমে 1 আর 3-এর স্থানবিনিময়, তারপর 2 আর 3-এর স্থানবিনিময় (Function composition-এর মত ডানদিক থেকে বাঁদিকে পড়ছি)। ফলে দাঁড়াচ্ছে (Fig 15)--

$$(2,3)(1,3) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

এখানে কিন্তু cycle দুটো মোটেই disjoint নয়, তাই কে আগে কে পরে সেটা গুরুত্বপূর্ণ। যেমন Fig 16 দেখলেই বুঝবে যে--

$$(1,3)(2,3) = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

এবার আর প্রশ্নটায় ফিরে আসি। এখানে দুটো জিনিস জানতে চেয়েছে--এক, যে permutation-টা দিয়েছে সেটাকে product of transposition হিসেবে লেখা যায় কিনা, এবং দুই, সেটা unique কিনা। এর মধ্যে প্রথম প্রশ্নটার উত্তর হল "হ্যাঁ, যায়"। বস্তুতঃ, যেকোনো permutation-কেই product of transposition হিসেবে লেখা যায়। তার একটা কায়দা হল এইরকম--প্রথমেই দ্যাখো দ্বিতীয় লাইনে 1 কার তলায় আছে। উত্তর হল 9-এর। ব্যস্ অমনি তুমি $(1,9)$ লাগাও (মানে 1 আর 9-এর স্থানবিনিময় করে দাও। সুতরাং 1 জায়গামত চলে গেল। এবার একইভাবে 2-কে জায়গামত নিয়ে যাও (ওর জায়গায় অন্য কিছু থাকলে তার সাথে স্থানবিনিময় করে)। এইভাবে করতে থাকলে পাবে Fig 17. যেসব সংখ্যা জায়গামত পৌঁছে গেছে তাদের মোটা করে দেখিয়েছি। এবার পরপর লিখে দিলেই হবে (ডান দিক থেকে বাঁদিকে লিখতে হবে কিন্তু!)--

Here one way of writing γ as a product of transpositions is

$$\gamma = (8,9)(5,8)(4,6)(3,7)(2,7)(1,7).$$

এবার দ্বিতীয় প্রশ্ন--এভাবে লেখাটা unique কিনা। আন্দাজ করতে পারছ হয়তো যে, unique নয়। এখানে আমরা প্রথমে 1-কে, তারপর 2-কে, এইভাবে জায়গামত আনছিলাম। যদি আমরা অন্যভাবে করতাম, যেমন প্রথমে 6-কে জায়গামত আনতাম, তারপর 5-কে, তারপর 4-কে, ইত্যাদি তবেই transposition-গুলো অন্যরকম হত। করেই দ্যাখো! ■

5.3 Symmetric group: S_n

ধরো কোনো একটা $n \in \mathbb{N}$ নিলাম। তাহলে $1, 2, ..., n$, এই n-খানা সংখ্যাকে কতভাবে সাজানো যায়? উত্তর হল $n!$ ভাবে। তার মানে মোট $n!$-খানা permutation পাওয়া যাচ্ছে। এদের set-টাকে লেখে S_n, যেমন S_3-র $3! = 6$ জন সদস্য হল--

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

আমরা এক্ষুণি দেখেছি যে, দুটো permutation-এর composition নিলে আরেকটা permutation পাওয়া যায়। তার মানে composition হল S_n-এর উপর একটা binary operation. একটু চিন্তা করলেই বুঝবে যে, $(S_n, \circ)$ হল একটা group

(এখানে $\circ$ মানে composition). কেন? কারণ প্রত্যেকটা permutation-ই হল $\{1, ..., n\}$ থেকে $\{1, ..., n\}$-এ একটা bijection. যে কোনো set-এর উপর যাবতীয় bijection-রা মিলে একটা group হয়, কারণ--

- দুটো bijection-এর composition একটা bijection হয়,
- identity function-টা একটা bijection,
- কোনো bijection-এর inverse-ও bijection হয়।

এখানে বিশেষভাবে গুরুত্বপূর্ণ হল identity element-টা, এক্ষেত্রে যার আরেকটা নাম identity permutation–

$$e = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix}.$$

সহজ ভাষায় identity permutation মানে সবাই যে যার জায়গায় গ্যাঁট্ হয়ে বসে আছে।

Example 41: True or false: The symmetric group S_3 is a commutative group.[2] **(2002)**

SOLUTION:

> The statement is false.
> Take
> $$\pi = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \in S_3.$$
> Then
> $$\pi\tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$
> while
> $$\tau\pi = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \neq \pi\tau.$$

■

Example 42: True or false: Every group of order 6 is a commutative group.[2.5] **(1999,2007)**

SOLUTION: এই অংকটা আসলে ছদ্মবেশে আগের অংকটাই। আমরা জানি যে S_n একটা group যার সাইজ $n!$. সুতরাং S_3-র সাইজ হল $3! = 6$. আর আমরা আগের অংকেই দেখেছি যে S_3 মোটেই commutative নয়। সুতরাং এই অংকের statement-টা false. আর আগের অংকের সমাধানটাই তার প্রমাণ। ■

5.4 Equations

আমরা গত অধ্যায়ে group-এর মধ্যে একটা equation কী করে solve করতে হয় শিখেছিলাম। এবার সেই কাজই আবার করব, খালি একটা বিশেষ ধরণের group-এর ক্ষেত্রে--S_n.

Example 43: $a = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$, $b = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ are two elements of S_3. Find the solution of the equation $ax = b$ in S_3.[3] **(2010.8d)**

SOLUTION:

The solution to $ax = b$ is $x = a^{-1}b$.

Now

$$a^{-1} = \begin{pmatrix} 3 & 2 & 1 \\ 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

এখানে a^{-1} বার করার জন্য a-র উপরের লাইনটাকে নীচে, আর নীচের লাইনটাকে উপরে নিয়ে গেলাম, এবং তারপর এখন যে লাইনটা উপরে আছে সেটাকে $1, 2, 3$ করে সাজিয়ে লিখলাম (তালে তালে নীচের সংখ্যাগুলোও স্থান পরিবর্তন করল)।

So

$$\begin{array}{c|ccc} & 1 & 2 & 3 \\ b & & & \\ & 1 & 3 & 2 \\ a^{-1} & & & \\ & 3 & 1 & 2 \end{array}$$

So the required solution is

$$x = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

■

Example 44: In the symmetric group S_4 of degree 4 solve the equation

$$x \circ (1 \quad 2 \quad 3) = (2 \quad 4 \quad 3),$$

where $\circ$ represents the composition of permutations.[2] **(2006,2014)**

SOLUTION:

Let

$$a = (1 \quad 2 \quad 3) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$$

and

$$b = (2 \quad 4 \quad 3) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}.$$

We are given $x \circ a = b$.

So $x = b \circ a^{-1}$.

Now

$$a^{-1} = (3 \quad 2 \quad 1) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}.$$

Cycle notation-এ inverse করা মানে হল cycle-এর সদস্যদের উল্টো করে লেখা।

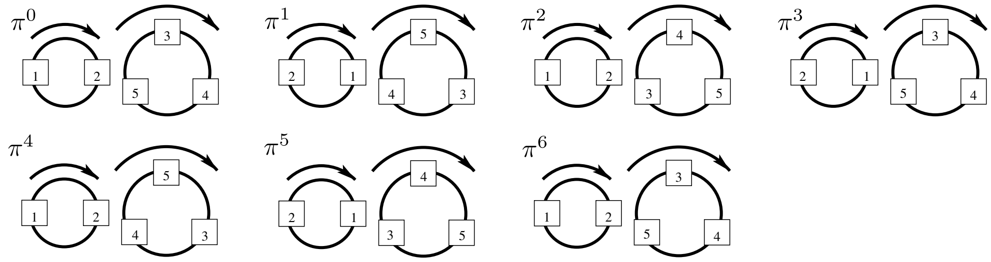


Fig 18

Also

$$\begin{array}{c|cccc} a^{-1} & 1 & 2 & 3 & 4 \\ & 3 & 1 & 2 & 4 \\ b & & & & \\ & 2 & 1 & 4 & 3 \end{array}$$

So

$$x = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = (1\ 2)(3\ 4).$$

উত্তরটা $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$ আকারে রাখলেই চলত, কিন্তু যেহেতু a আর b-কে cycle notation-এ দিয়েছে, তাই উত্তরটাকেও cycle দিয়ে লিখলাম। ■

5.5 Order

Group theory-তে order শব্দটার মানে কী, সেটা আমাদের অপরিচিত নয়। গত অধ্যায়েই শিখেছি যে, এটা দুই অর্থে ব্যবহৃত হয়--

- একটা group-এর order মানে তাতে কতগুলো element আছে (অর্থাৎ সাইজ)।
- আর g যদি group-টার একটা element হয়, তবে তার order মানে সবচেয়ে ছোটো $k \in \mathbb{N}$ যাতে $g^k = e$ হয়। যদি এরকম $k \in \mathbb{N}$ না পাওয়া যায়, তবে order বলি ∞.

এবার যে অংকগুলো করব তাতে অনেক সময়ে একটা permutation-এর order বার করতে বলবে। এখানে order শব্দটা দ্বিতীয় অর্থে ব্যবহার হচ্ছে--আমাদের group-টা হল S_n এবং permutation-টা হল তার একটা element. সুতরাং তার order হল সবচেয়ে ছোটো $k \in \mathbb{N}$ যাতে ওই একই permutation পরপর k বার করলে সবকিছু গোড়ার অবস্থানে ফিরে আসে।

Example 45: Define order of a permutation.[1] **(2009)**

SOLUTION:

> DEFINITION: **Order of permutation**
>
> By the order of a permutation π we mean the least positive integer n such that π^n is the identity permutation.

■

কয়েকটা উদাহরণ নিই।

Example 46: যদি $\pi = (1,3) \in S_3$ হয়, তবে $o(\pi) = ?$

SOLUTION: এখানে π হল সেই permutation, যেটা 1 আর 3-এর স্থানবিনিময় করে। বুঝতেই পারছ দুবার এরকম ওল্টালে আমরা আবার মূল অবস্থানে ফিরে আসব। সুতরাং $o(\pi) = 2$. ■

একই যুক্তিতে যে কোনো cycle-এরই order হবে তার দৈর্ঘ্য, যেমন $r = (1,3,2)$ হলে $o(r) = 3$. এবার একটা একটু জটিল উদাহরণ দেখি, যেটা শিখলেই তুমি বুঝে যাবে কীভাবে যে কোনো permutation-এর order বার করতে হয়।

Example 47: একটা permutation দিচ্ছি cycle notation-এ, $\pi = (1,2)(3,4,5)$. এর order কত হবে?

SOLUTION: Fig 18 দ্যাখো। এখানে cycle দুটোকে দুটো চাকার মত দেখিয়েছি। প্রতিবার π লাগালে চাকাদুটো একঘর করে ঘুরবে। প্রথম চাকাটা প্রতি দুবারের মাথায় গোড়ার অবস্থানে ফিরে আসছে। দ্বিতীয় চাকাটা ফিরে আসছে প্রতি তিনবারের মাথায়। সুতরাং কখন $\pi^k = e$ হবে, মানে দুটো চাকাই একই সঙ্গে শুরুর অবস্থানে ফিরে আসবে? উত্তর হল--যখন k সংখ্যাটা 2 আর 3 দুটো দিয়েই ভাগ যাবে। আমরা এরকম সবচেয়ে ছোটো $k \in \mathbb{N}$ খুঁজছি। সেটা হবে 2 আর 3-এর LCM (লসাগু), মানে 6. ■

এই উদাহরণটা পড়ার পর নীচের theorem-টা নিয়ে কোনো সন্দেহের অবকাশ নেই।

THEOREM

Let $\pi = c_1 c_2 \cdots c_p$ be a permutation where $c_1, ..., c_p$ are disjoint cycles. Then

$$o(\pi) = LCM(o(c_1), ..., o(c_p)).$$

যেমন উদাহরণটায় $c_1 = (1,2)$ আর $c_2 = (3,4,5)$ ছিল, তাই $o(c_1)$ হল c_1-এর দৈর্ঘ্য মানে 2, আর একইভাবে $o(c_2) = 3$.
এবার নীচের অংক কয়টা কর দেখি। সাবধান, শেষের অংকটায় কিন্তু সামান্য প্যাঁচ আছে!

Exercise 14: Find the orders of the following permutations:
(1) $(1,3,10)(2,4,5)$, **(2)** $(1,3)(2,4)$, **(3)** $(1,2)(2,3,4)$.
■

যে কোনো permutation-এর order বার করার সহজ কায়দা হল প্রথমে cycle notation-এ লিখে ফেলা, এবং theorem-টা লাগানো।

Example 48: Determine the order of the permutation

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}.$$

[2] **(2009)**
SOLUTION: প্রথমে এটাকে cycle notation-এ লিখে ফেলব--

> In cycle notation the given permutation is
> $$(1, 3, 2).$$

একটাই cycle আছে, সুতরাং LCM বার করার ঝামেলাও নেই, খালি cycle-টার দৈর্ঘ্য নিলেই হবে।

> We know that the order of a cycle equals its length.
> So the required order is 3.

■

Example 49: Find the order of the permutation

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 4 & 2 & 3 & 1 & 7 & 8 & 6 \end{pmatrix}.$$

[2] **(2011.8c)**
SOLUTION:

> In cycle notation the permutation is
> $$(1, 5)(2, 4, 3)(6, 7, 8).$$
> So it is product of 3 cycles of lengths 2, 3 and 3.
> Hence the required order is the LCM of the cycle lengths
> $$LCM\{2, 3, 3\} = 6.$$

■

Example 50: Prove that a finite group G of order n is cyclic if and only if there exists an element b in G such that the order of b is n. Use this result to show that the symmetric group S_3 is not cyclic.[3+2] **(2009.7b)**

Fig 19

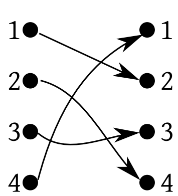


Fig 20

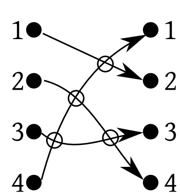
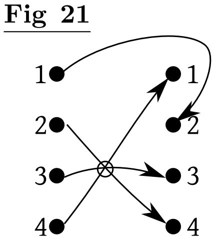


Fig 21



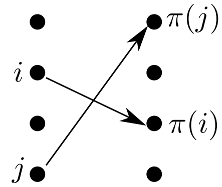


Fig 22

SOLUTION: এই অংকের প্রথম অংশটা তো আগেই করেছি Example 25-এ। এবার দ্বিতীয় অংশে দেখাতে বলেছে যে, S_3 একটা cyclic group নয়। আমরা জানি যে S_3 আদৌ commutative-ই নয়। সুতরাং cyclic আর হবে কী করে? Cyclic group মাত্রেই তো commutative হয়! কিন্তু এই অংকটায় অত সহজে পার পাওয়া যাবে না। এখানে সরাসরি প্রমাণ চায় নি, বলে দিয়েছে প্রথম অংশটা ব্যবহার করে দেখাতে হবে। তার মানে ধরে ধরে প্রত্যেকটা element-এর order পরীক্ষা করে দেখাতে হবে যে order-গুলো সবাই $|S_3| = 6$-এর চেয়ে ছোটো--

> We know that
>
> $$S_3 = \{\ e,\ \ (1,2),\ \ (2,3),\ \ (3,1),\ \ (1,2,3),\ \ (1,3,2)\ \}.$$

এটা আসলে সেই ত্রিভুজের উদাহরণটাই। যেমন $(1,2)$ মানে 3-কে স্থির রেখে $1,2$-এর স্থানবিনিময়, যাকে আমরা f_3 বলেছিলাম। একইভাবে $(1,2,3)$ হল ℓ.

> We also know that $o(e) = 1$ for any group, and the order of a cycle equals its length.
>
> Since none of the cycles has length 6,
>
> so no element of S_3 has order equal to $|S_3| = 6$.
> So S_3 is not a cyclic group.

■

DAY 6
Permutation groups (part 2)

6.1 Even এবং odd permutation

S_n-এর মধ্যে মোট $n!$-খানা permutation আছে, এদের দুটো সমান ভাগে ভাগ করা যায়, একটা ভাগের সদস্যদের বলে **even permutation**, অন্যদের বলে **odd permutation**.
সংজ্ঞাটা একটু অদ্ভুত। একটা উদাহরণ দিয়ে বুঝি।

Example 51: ধরো বার করতে হবে এই permutation-টা even নাকি odd–

$$\begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 4 & 3 & 1\end{pmatrix}.$$

SOLUTION: প্রথমে এটাকে একটা function হিসেবে তীর চিহ্ন দিয়ে এঁকে নাও (Fig 19)। এবার দ্যাখো তীরগুলোর মধ্যে কতগুলো ক্রসিং আছে, মানে এরকম কত জোড়া তীর আছে, যাদের গোড়াগুলো যে ক্রমে আছে ডগাগুলো আছে তার উল্টো ক্রমে। Fig 20 দেখলেই বুঝবে যে সংখ্যাটা হল 4, যেটা একটা even সংখ্যা। তাই এটা একটা even permutation. অবশ্য তুমি এখানে আপত্তি তুলতেই পারো এই বলে যে, যদি তীরগুলো কায়দা করে আঁকতাম (ধরো, Fig 21-এর মত করে), তবে তো ক্রসিংএর সংখ্যা মনে হচ্ছে খালি 1, যেটা odd সংখ্যা। তাহলে? আসলে even বা odd permutation বার করার জন্য তীরগুলোকে কখনও বাইরে থেকে ঘুরিয়ে আনা যাবে না (যেমন Fig 21-এ 1 থেকে বেরোনো তীরটা করেছে)। আর দুয়ের বেশী তীর যেন একটা বিন্দু দিয়ে না যায়। মানে সহজ বুদ্ধিতে তীর আঁকলে যেমন হবে সেইভাবেই আঁকতে হবে। ■

যাই হোক, অংকের সংজ্ঞা লেখার সময়ে এরকম "সহজ বুদ্ধি-টহজ বুদ্ধি"-র কোনো মানে হয় না। তাই অংকের ভাষায় লেখার সময়ে আমরা ক্রসিংএর (যাকে অংকের ভাষায় inversion বলে), তার সংজ্ঞা লিখব এইভাবে--

> DEFINITION: **Inversion**
>
> Let $\pi \in S_n$. Then $\{i,j\} \subseteq \{1,...,n\}$ is called an **inversion** in π, if $i<j$ but $\pi(i)>\pi(j)$.

এখানে $i<j$ মানে প্রথম তীরটার গোড়া রয়েছে দ্বিতীয় তীরের গোড়ার উপরে, , আর $\pi(i)>\pi(j)$ মানে প্রথম তীরের ডগা চলে গেছে দ্বিতীয় তীরের ডগার নীচে। Fig 22 দ্যাখো।

Example 52: $\pi = \left(\begin{smallmatrix}1 & 2 & 3 & 4\\ 4 & 2 & 1 & 3\end{smallmatrix}\right)$-তে $\{1,2\}$ কি একটা inversion? $\{3,4\}$? আর $\{4,3\}$?

SOLUTION: প্রথমে $\{1,2\}$ নিয়ে কাজ করি। এখানে $1<2$, কিন্তু $\pi(1)=4>2=\pi(2)$. সুতরাং $\{1,2\}$ একটা inversion.
তবে $\{3,4\}$ মোটেই একটা inversion নয়, কারণ $3<4$ এবং $\pi(3)=1<3=\pi(4)$.
$\{4,3\}$ আসলে $\{3,4\}$-ই। এখানে আমরা set নিয়ে আলোচনা করছি, তাই কে আগে কে পরে তাতে কিছু এসে যায় না। সুতরাং $\{4,3\}$-ও অবশ্যই inversion নয়। ■

এবার তবে আমরা even এবং odd permutation-এর সংজ্ঞা লিখে ফেলতে পারি।

> DEFINITION: **Even and odd permutation**
>
> A permutation is called **even** (or **odd**) if the total number of inversions in it is even (or odd).

নীচের অংকটা করে একটু গা গরম করে নাও, যাতে একটা permutation দেওয়া থাকলে সেটা even নাকি odd বার করতে অসুবিধা না হয়।

Example 53: Is the permutation

$$\alpha = \begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9\\ 3 & 5 & 2 & 9 & 1 & 7 & 6 & 4 & 8\end{pmatrix}$$

an even permutation on I_9? Justify your answer. **(1999)**

SOLUTION: এখানে কাজটা ছবি এঁকে করাই যায়, কিন্তু লিখে করাটাও খুবই সহজ। Permutation-টা double decker notation-এর আছে, যেখানে উপরের লাইনে সংখ্যাগুলো ছোটো থেকে বড় পরপর সাজানোই রয়েছে। এবার নীচের লাইনে একেবারে বাঁদিক থেকে শুরু কর। সেখানে আছে 3. খেয়াল কর 3-এর চেয়ে ছোটো কতগুলো সংখ্যা 3-এর ডানদিকে চলে গেছে। এখানে এরকম দুটো আছে, 1 আর 2. এরা প্রত্যেকে একটা করে inversion-এর জন্ম দেবে। প্রথমে দেখি 2-টা 3-এর ডানদিকে চলে যাওয়ায় কী inversion হয়েছে। Double decker notation-এর 3-এর উপরে আছে 1, আর 2-এর উপরে আছে 3. তাই inversion-টা হবে $\{1,3\}$. একইভাবে 1-টা 3-এর ডানদিকে চলে যাওয়ায় যে inversion-টা পাচ্ছ, সেটা হল $\{1,5\}$.

3 নিয়ে কাজ হয়ে গেল। এবার 3-এর পরে আছে 5. খুঁজে দ্যাখো 5-এর ডান দিকে 5-এর চেয়ে ছোটো কী কী সংখ্যা রয়েছে। উত্তর হল 2, 1 আর 4. এদের দরুণ এই তিনটে inversion পাবে--$\{2,3\},\{2,5\}$ আর $\{2,8\}$.

এইভাবে চালিয়ে গেলে--

> By inspection the inversions in α are
>
> $$\begin{aligned} \{1,3\},\{1,5\}, \\ \{2,3\},\{2,5\},\{2,8\}, \\ \{3,5\}, \\ \{4,3\},\{4,6\},\{4,7\},\{4,8\},\{4,9\}, \\ \{6,7\},\{6,8\}, \\ \{7,8\}. \end{aligned}$$
>
> The total number of inversions is 14, which is even.
>
> $\therefore \alpha$ is an even permutation.

■

কোনো permutation-কে cycle notation-এ লিখে নিলে সেটা even নাকি odd বার করা খুব সহজ হয়। একটা cycle কীরকম হবে, even নাকি odd, সেটা তার দৈর্ঘ্যের উপর নির্ভর করে। দৈর্ঘ্য যদি odd হয়, তবে cycle-টা even হবে। দৈর্ঘ্য যদি even হয়, তবে cycle-টা হবে odd. যেমন $(1,7,3)$-এর দৈর্ঘ্য হল 3, যেটা odd. সুতরাং cycle-টা even হবে। যদি একাধিক cycle থাকে, তবে even, odd-গুলো যোগ হয়ে যায়, এই নিয়ম অনুযায়ী--

even + even = even,

odd + odd = even এবং

even + odd = odd.

এগুলো আলাদা করে মুখস্থ রাখার কোনো দরকার নেই। এগুলো সাধারণ সংখ্যার যোগের নিয়মের মতই, যেমন দুটো বিজোড় সংখ্যা যোগ করলে যোগফল সর্বদাই একটা জোড় সংখ্যা হয়।

এই কায়দায় আগের অংকটাই আরেকবার করা যাক--

Example 54: Is the permutation

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 5 & 2 & 9 & 1 & 7 & 6 & 4 & 8 \end{pmatrix}$$

an even permutation on I_9? Justify your answer. **(1999)**

SOLUTION:

> In disjoint cycle notation the permutation is
>
> $$(1\ 3\ 2\ 5)(4\ 9\ 8)(6\ 7).$$
>
> The cycles are of length even, odd, even.
>
> So their parities are odd, even, odd.

Parity মানে odd বা even হওয়ার ব্যাপারটা, যেমন পুরুষ বা মহিলা হওয়ার ব্যাপারটাকে লিঙ্গ বলে।

> So the parity of α is
> odd + even + odd = even.
> Thus, the given permutation is even.

■

Exercise 15: The permutation

$$\delta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 1 & 7 & 6 & 10 & 4 & 2 & 5 & 9 & 8 \end{pmatrix}$$

on the set $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ is an even permutation.[2] **(2001)** ■

Example 55: For the permutations

$$A = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix} \text{ and } B = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 4 & 5 & 2 \end{pmatrix}$$

find AB. What is the parity of AB?[2+1] **(2002)**

SOLUTION: প্রথম অংশ আগেই করেছি Example 39-এ। সেখানেই দেখেছিলাম যে--

> $$AB = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 4 & 3 \end{pmatrix}.$$

এবার এর parity বার করব।

> In disjoint cycle notation
>
> $$AB = (1\ 2)(3\ 5),$$
>
> which is a product of two even length (hence odd parity) cycles. So the parity of AB is odd+odd = even.

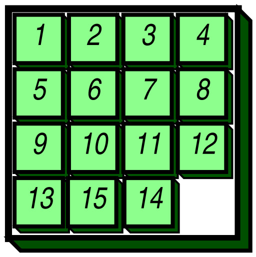


Fig 23

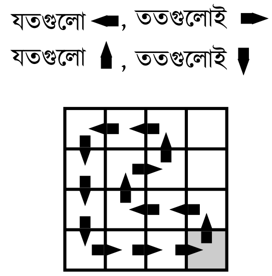


Fig 24

■

Exercise 16: If $\alpha = (1\ 3\ 4)(5\ 6)(2\ 7\ 8\ 9)$ and

$$\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 8 & 9 & 6 & 4 & 5 & 2 & 3 & 1 \end{pmatrix}$$

are two permutations, find the product $\gamma = \beta^{-1}\alpha\beta$. Is γ an even permutation? **(2012)**

HINT:

■

Example 56: Find A^2, A^{-1} for the permutation

$$A = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}.$$

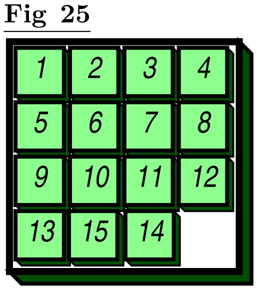
Is A^{-1} an even permutation? Justify.[1+2+1] **(2000)**

SOLUTION:

We have

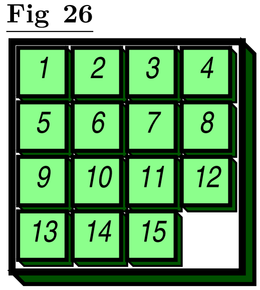
$$\begin{aligned} A^2(1) &= A(A(1)) = A(1) = 1, \\ A^2(2) &= A(A(2)) = A(3) = 4, \\ A^2(3) &= A(A(3)) = A(4) = 2, \\ A^2(4) &= A(A(4)) = A(2) = 3. \end{aligned}$$

Fig 25



1, 2, ...,13, 15, 14, 16

Fig 26



1, 2, ...,13, 14, 15 , 16

So

$$A^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}.$$

Also interchanging the two lines of A we have

$$A^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}.$$

In disjoint cycle notation

$$A = (2\ 3\ 4),$$

which is a cycle of odd length, and so has even parity.

■

Example 57: $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 4 & 7 & 5 & 2 & 3 & 1 \end{pmatrix}$. Is f^{-1} an odd permutation? Justify your answer.[2] **(2010.8c)**

SOLUTION:এটা নিজে নিজে চেষ্টা কর। এরকম অংক একটু আগেই করেছি।

■

6.1.1 15-puzzle

প্রথম অধ্যায়ে স্যাম লয়েডের 15 puzzle-এর কথা মনে আছে? সেই যেটার সমাধান করতে গিয়ে সবাই খাবি খাচ্ছিল (Fig 23)? এবার শিখব কিভাবে সেটার মোকাবিলা করতে হয়। তার জন্য প্রথমে একটা ছোট্টো (কিন্তু গুরুত্বপূর্ণ) জিনিস লক্ষ কর। যদি π যেকোনো একটা permutation হয় এবং এদের মধ্যে যে কোনো দুটো সংখ্যার স্থানবিনিময় কর তবে একটা নতুন permutation পাবে। এরকম দুজনের মধ্যে স্থানবিনিময় করাকে বলে একটা **transposition**.

যেমন ধরো যদি $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 3 \end{pmatrix}$ হয়, তবে 1 আর 3-এর transposition করলে হবে $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 3 & 1 \end{pmatrix}$. লক্ষ কর এখানে যে 1 আর 3 ব্যবহার করেছি তারা নীচের তলার সংখ্যা। অর্থাৎ 1 সংখ্যাটার সঙ্গে 3 সংখ্যাটার বিনিময় করেছি। ভুল করে যেন উপরের তলার 1 আর 3-এর স্থান বিনিময় করে বোসো না।

এবার আমরা স্যাম লয়েডের ধাঁধাটাকে শায়েস্তা করব দুই ধাপে--

প্রথমে লক্ষ কর যে ফাঁকা জায়গাটা শুরুতে যেখানে ছিল শেষেও সেখানেই আছে। তার মানে তুমি যতই যা কর না কেন, ফাঁকা জায়গাটাকে আবার তার বাড়িতে ফিরিয়ে দিতে হবে। সুতরাং যদি কখনও ফাঁকা জায়গাটা k ঘর ওপরে ওঠে তবে ওকে ফের ঠিক k ঘর নামিয়ে আনতে হবে। সুতরাং ওঠানামা জাতীয় চালের মোট সংখ্যা হবে $2k$, যেটা একটা even সংখ্যা। Fig 24 দ্যাখো। একই যুক্তি খাটবে ডাইনেবাঁয়ে সরার ক্ষেত্রেও। ঠিক যতঘর বাঁয়ে যাবে, তত ঘরই ডাইনে ফিরতে হবে। সুতরাং ডাইনেবাঁয়ে চালের সংখ্যাও হবে even. সুতরাং মোট চালের সংখ্যা even হতে বাধ্য। প্রথম ধাপের সিদ্ধান্ত তাহলে পেলাম এই--

> ধাঁধাটার সমাধান যদি করতেই হয়, তবে সেটা even-সংখ্যক চাল দিয়েই করতে হবে।

এবার দ্বিতীয় ধাপ--তুমি সবগুলো গুটিকে পরপর সাজিয়ে ফ্যালো, প্রথমে ওপরের লাইন, তারপর দ্বিতীয় লাইন, ঠিক যেভাবে আমরা পড়ি। ফাঁকা ঘরটাকে বল 16 নম্বর গুটি। তাহলে প্রাথমিক অবস্থানে তুমি $1, ..., 16$-র একটা permutation পাবে (Fig 25)। এটা S_{16}-এর একটা element. একটু চিন্তা করলেই বুঝবে যে এখানে খালি একটাই inversion আছে (ওই 14 আর 15 উল্টে আছে বলে), তাই এটা একটা odd permutation. একইভাবে শেষ অবস্থানের গুটিগুলোকে সাজালে পাবে Fig 26-এর মত permutation. এখানে কোনো inversion নেই। সুতরাং এটা একটা even permutation.

এবার তুমি প্রাথমিক অবস্থান থেকে শুরু করে একটা কিছু চাল দাও। তার মানে ফাঁকা জায়গাটাকে কোনো একদিকে সরাবে, আর যে ঘরে সরাবে, সেখানকার গুটিটাকে নিয়ে আসবে এখনকার ফাঁকা জায়গাটায়। অর্থাৎ, কোনো একটা গুটির সঙ্গে আমাদের 16 নম্বর গুটির স্থানবিনিময় হবে, অর্থাৎ transposition. সুতরাং যাই চাল দাও না কেন নতুন permutation-টা একটা even permutation হতে বাধ্য। একই কথা খাটবে তার পরের চালেও। সুতরাং দুই চাল পরে তুমি ফের একটা odd permutation পাবে। তিন চালের মাথায় even এবং চার চালের মাথায় ফের odd permutation. এইভাবে odd,even,odd,even করে চলতে থাকবে। সুতরাং দ্বিতীয় ধাপের সিদ্ধান্ত হল--

> even সংখ্যক চালের পরে তোমাকে odd permutation-এই থাকতে হবে।

এদিকে তোমার কাজ তো হল একটা even permutation-এ পৌঁছনো। প্রথম ধাপ থেকে জানি যে কাজটা করতে হবে even সংখ্যক চাল দিয়েই। বুঝতেই পারছ যে সেটা অসম্ভব। অর্থাৎ স্যাম লয়েডের ধাঁধাটা করা অসম্ভব। যাই হোক, এই সত্যটা ফাঁস হবার আগেই স্যাম লয়েড ধাঁধাটা বিক্রী করে প্রচুর মুনাফা করে নিয়েছিলেন।

6.1.2 Even-odd-এর নামতা

আমরা permutation-দের বিষয়ে দুটো গুরুত্বপূর্ণ জিনিস শিখেছি--এক, ওরা দুই ধরণের হয়, even আর odd, এবং দুই, transposition-এর ফলে even-গুলো odd এবং odd-গুলো even হয়ে যায়। এবার একটা তৃতীয় জিনিস শিখব--যে কোনো permutation থেকে তুমি যেকোনো permutation-এ পৌঁছতে পারো, কেবলমাত্র বারবার transposition লাগিয়ে। কাজটা খুবই সহজ।

Example 58: একটা উদাহরণ দিয়ে দেখলেই বুঝবে। ধরো একটা permutation হল $4,5,6,3,1,2$. এখানে থেকে তোমাকে পৌঁছতে বললাম $5,3,2,4,1,6$-এ। কাজটা করতে হবে খালি পরপর transposition করে করে। কি করে এগোবে?

SOLUTION: প্রথমে দ্যাখো 1-টা কোথায় আছে। দুই ক্ষেত্রেই 1 আছে 5 নম্বর স্থানে। সুতরাং 1-কে নিয়ে কোনো সমস্যা নেই। এবার দ্যাখো 2 কোথায় আছে। শুরুতে আছে 6 নম্বরে, নিয়ে যেতে হবে 3 নম্বরে। সুতরাং 6 নম্বর আর 3 নম্বর স্থানবিনিময় কর। তবে পেলে $4,5,2,3,1,6$. এবার দ্যাখো 3 কোথায় আছে। এখন আছে 4 নম্বর স্থানে, নিতে হবে 2 নম্বরে। অতএব 4 নম্বর আর 2 নম্বর স্থানবিনিময় করব, পাব--$4,3,2,5,1,6$. বুঝতেই পারছ এভাবে প্রতি ধাপে আমরা একটা করে সংখ্যাকে যথাস্থানে পাঠাতে পারব। ■

যে ভাবে আমরা কাজটা করলাম সেটাই একমাত্র পদ্ধতি নয়, নানাভাবেই করা যেত। কিন্তু স্যাম লয়েডের ধাঁধার ক্ষেত্রে আমরা যে যুক্তি দিয়েছিলাম, সেই যুক্তিতেই এটা বোঝা যায় যে কোনো even permutation থেকে শুরু করে কেবলমাত্র transposition ব্যবহার করে কোনো odd permutation-এ যেতে হলে আমাদের পক্ষে odd সংখ্যক transposition ব্যবহার করা ছাড়া গত্যন্তর নেই। একইরকম কথা odd থেকে even-এর ক্ষেত্রেও বলা যায়। তেমনি odd থেকে odd, বা even থেকে even-এ যেতে হলে ঠিক even-সংখ্যক transposition-ই লাগবে।
লক্ষ কর যে identity permutation হল একটা even permutation. সুতরাং identity permutation থেকে যদি কোনো even permutation-এ যেতে চাও কেবলমাত্র transposition ব্যবহার করে, তবে ঠিক even-সংখ্যক transposition-ই লাগবে। ধরো π একটা even permutation, এবং identity থেকে π-তে পৌঁছতে আমরা $2k$-খানা transposition ব্যবহার করেছি--প্রথমে (i_1, j_1),তারপর (i_2, j_2), এইভাবে চলতে চলতে সবশেষে (i_{2k}, j_{2k}). তার মানে

$$\begin{aligned}\pi &= (i_{2k}, j_{2k})(i_{2k-1}, j_{2k-1})\cdots(i_1, j_1)e\\ &= (i_{2k}, j_{2k})(i_{2k-1}, j_{2k-1})\cdots(i_1, j_1).\end{aligned}$$

এ থেকে আমরা একটা দরকারী জিনিস জানতে পারলাম--যেকোনো even permutation-কেই even-সংখ্যক transposition-এর product হিসেবে লেখা যায়। একইরকম যুক্তিতে বলতে পারি যে, যে কোনো odd permutation-কে odd-সংখ্যক transposition-এর product হিসেবে লেখা যায়। এর উল্টোটাও সত্যি। সেটাকে একটা theorem হিসেবে লিখে নিই।

THEOREM

A permutation $\pi \in S_n$ is an even permutation if and only if it can be expressed as the product of an even number of transpositions. Equivalently, a permutation is an odd permutation if and only if it can be expressed as the product of an odd number of transpositions.

এই theorem-টা থেকে এক গুচ্ছ কাজের জিনিস পাওয়া যায়--

1. যদি π, λ দুটো even permutation হয়, তবে $\pi\lambda$-ও একটা even permutation-ই হবে।
2. যদি π একটা even permutation হয়, তবে π^{-1}-ও তাই হবে।

তালিকাটাকে আরো লম্বা করা যায়, কিন্তু পাছে ব্যাপারটা বিরক্তিকর হয়ে পড়ে, তাই বাকিগুলোকে নীচের অংকটার মধ্যে ঢুকিয়ে দিলাম।

Exercise 17: ধরো $\pi, \lambda \in S_n$. আমরা দেখতে চাই π আর λ কি রকম permutation (মানে even না odd) জানা থাকলে তা থেকে সব সময়ে $\pi\lambda$-র parity বলে দেওয়া যায় কি না। সেই অনুযায়ী নীচের টেবিলটা পূর্ণ কর।

	π even	π odd
λ even	even	
λ odd		

π আর λ দুজনেই even হলে $\pi\lambda$-ও even-ই হয়, সেটা টেবিলে ঢুকিয়ে দিয়েছি। বাকি তিন জায়গায় কি কি বসবে? ■

এবারের অংকটার সমাধান খুবই সংক্ষিপ্ত, কিন্তু একটু মাথা খাটাতে হবে।

Exercise 18: আমরা গোড়াতেই বলেছিলাম যে S_n-এর যে কোনো element-ই হয় even নয় odd. সেটা তো দেখলামই। কিন্তু আরও একটা কথা বলেছিলাম--even এবং odd permutation-দের সংখ্যা সমান। এটা কিন্তু এখনও প্রমাণ করি নি। প্রমাণ করতে পারো?

HINT:

সমাধানটা তুমিই করবে, খালি শুরুটা একটু ধরিয়ে দিই। ধরো S_n-এর মধ্যে even permutation-দের set-টাকে A নাম দিলাম, আর odd-দের set-টাকে বললাম B. তোমাকে দেখাতে হবে যে A আর B-এর সাইজ সমান। দুটো set-এর সাইজ সমান দেখানোর কায়দা তো জানোই--A থেকে B-তে একটা bijection দেখানো। এবার ভেবে দ্যাখো কি bijection নেবে! এরকম অনেক bijection আছে কিন্তু! ■

Exercise 19: একটা odd permutation-এর inverse কি সব সময়েই একটা odd permutation হবে? ■

6.2 Subgroups

Example 59: In the symmetric group S_3 show that the subsets

$$A = \{e, (1\ 2)\} \text{ and } B = \{e, (1\ 2\ 3), (1\ 3\ 2)\}$$

are subgroups. Use Lagrange's theorem to show that $A \cup B$ is not a subgroup of S_3. Here e is the identity of S_3.[4] **(1997)**

SOLUTION:

> Since $(1\ 2)^2 = e$ we see that A is the subgroup of S_3 generated by $(1\ 2)$.
>
> Also, since $(1\ 2\ 3)^2 = (1\ 3\ 2)$ and $(1\ 2\ 3)^3 = e$, we see that B is the subgroup of S_3 generated by $(1\ 2\ 3)$.
>
> $|A \cup B| = 5 \not| 6 = |S_3|$. So by Lagrange's theorem, $A \cup B$ cannot be a subgroup of S_3.

■

Example 60: In the symmetric group S_3 find two subgroups A and B such that $A \cup B$ is not a subgroup of S_3.[4] **(2001)**
SOLUTION: আগের অংকটাই। ■

Example 61: If $x = (1\ 2\ 3\ 4)$ then show that the set $\{x, x^2, x^3, x^4\}$ forms a cyclic group.[3] **(2010.7c)**
SOLUTION:

> We first notice that $o(x) = 4$.
>
> ⟦ Because:
>
> $x = (1\ 2\ 3\ 4)$,
> $x^2 = (1\ 3)(2\ 4)$,
> $x^3 = (1\ 4\ 3\ 2)$,
> $x^4 =$ identity.
>
> ⟧
>
> So $\forall n \in \mathbb{Z} \quad x^n = x^r$ where $r \in \{1, 2, 3, 4\}$ is such that $n \equiv r (\text{mod } 4)$.
>
> So $\{x, x^2, x^3, x^4\}$ is closed under multiplication and inverse. So it is a group.
>
> Also it is generated by a single element x.
>
> So it is cyclic.

■

6.2.1 Alternating subgroup, A_n

আমরা দেখলাম যে দুটো even permutation-এর product ফের even হয়, এবং even permutation-দের inverse-ও even হয়। সুতরাং--

> **THEOREM**
>
> The set of all even permutations in S_n forms a subgroup. It is called the **alternating subgroup,** and is denoted by A_n.

Exercise 20: বল তো A_3-র সাইজ কত? ■

Example 62: Show that A_3, the set of even permutations of $\{1,2,3\}$, is a group w.r.t. the product of permutations. Is it commutative? Answer with reason.[4+1] **(2004)**

SOLUTION:

> The set of all permutations of $\{1,2,3\}$ is
>
> $$e, \quad (2,3), \quad (1,3), \quad (1,2), \quad (1,2,3), \quad (1,3,2).$$
>
> Since cycles of even lengths are odd permutations and vice versa, the only three even permutations are
>
> $$e, \quad \ell = (1\ 2\ 3) \text{ and } r = (1\ 3\ 2).$$

ত্রিভুজের উদাহরণটা মাথায় থাকলে ব্যাপারটা বুঝতে সুবিধা হবে। সেখানে r মানে ছিল ডান দিকে এক ঘর ঘোরানো, আর ℓ মানে বাঁদিকে এক ঘর ঘোরানো।

> Since ℓ is a cycle of length 3, hence its order is 3.
>
> Also, by direct computation, $\ell^2 = r$.
>
> Thus $A_3 = \{e, \ell, r\} = \{\ell^0, \ell, \ell^2$ is the cyclic subgroup generated by ℓ.
>
> Hence A_3 is a group w.r.t. the product of permutations, as required.

এবার দ্বিতীয় অংশ--

> Since it is a cyclic subgroup, hence it is commutative.

■

আমরা দেখালাম A_3 একটা group. একইভাবে যে কোনো A_n-ই একটা group. এখানে একটা সাবধানবাণী দিয়ে রাখি--আমরা এটাও দেখালাম যে, A_3 হল commutative. সেটা কিন্তু যে কোনো A_n-এর জন্য খাটে না। বস্তুতঃ $n > 3$ হলেই A_n আর commutative থাকে না।

Exercise 21: Prove that the set of all even permutations of $\{1,2,3\}$ is a cyclic group. Determine two distinct generators of it.[4] **(2011.7b)**

HINT: আগের অংকেই প্রথম অংশের উত্তর রয়েছে। সেখানে আমরা ℓ-কে generator নিয়েছিলাম। চাইলে r-কেও নিতে পারতাম। তাই এই অংকের দ্বিতীয় অংশে ℓ আর r-কে দুটো distinct generator হিসেবে নেওয়া যাবে। ■

Example 63: Determine all distinct left cosets of A_3 in S_3.[3] **(2009.8bii)**

SOLUTION:

> We know that $|S_3| = 3! = 6$. Also exactly half of the 6 permutations are even. So $|A_3| = 6/2 = 3$.
>
> Hence A_3 has exactly $6/3 = 2$ cosets in S_3.
>
> One of the left cosets is S_3 itself. The remaining left coset consists of $S_3 \setminus A_3$.
>
> Thus, left coset A_3 : is $\{e, (1,2,3), (1,3,2)\}$, and the other left coset is $\{(1,2), (2,3), (1,3)\}$.

■

Exercise 22: যদি উপরের অংকটায় left coset-এর বদলে right coset বলত, তবে উত্তরটা কি পাল্টাত? ■

Answers

1. দ্বিতীয় সারিকে। **5.** $x \in [g]$ হলে $x^{-1}g \in H$, মানে $f(x) \in H$. সুতরাং f-টা সত্যিই $[g]$ থেকে H-এ একটা function. যদি $f(x_1) = f(x_2)$ হয়, তবে $x_1^{-1}g = x_2^{-1}g$. দু দিক থেকে g কেটে *inverse* নিলেই $x_1 = x_2$. তাই one-one. যদি $h \in H$ নাও তবে $x = gh^{-1} \in [g]$ নিলেই $f(x) = h$ হবে, তাই onto. **6.** হ্যাঁ।
11. **(1)** উপরতলায় দুবার 2 হবে না। **(2)** উপরতলার সংখ্যাগুলো $1, 2,$ করে পর লেখাই নিয়ম। সুতরাং 3 বাদ দিয়ে 4 আসাটা ঠিক নয়। **(3)** নীচের তলায় দুবার 1 হবে না। **12.** $A^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}$. $A^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}$.
14. **(1)** 12. **(2)** 2.4. এখানে cycle দুটো disjoint নয়। Cycle notation-এ লিখলে permutation-টা $(1, 2, 3, 4)$. **19.** হ্যাঁ। **20.** $|S_3| = 3! = 6$. সুতরাং $|A_3| = 6/2 = 3$. **22.** না।

Chapter IV
Rings and Fields (year 2)

DAY 7
Ring (part 1)

7.1 কেন এবং কী?

আগেকার দিনে মানুষ গান শুনত গ্রামোফোনে। মস্ত বড় চাকার মত রেকর্ডের গায় আঁচড় কেটে গানের সুরটা বসানো থাকত। যদি তার উপর ভুল করে কেউ অন্যরকম আঁচড় কেটে দিত তবে সেই রেকর্ড আর বাজত না।

তারপর এল টেপ রেকর্ডার আর ক্যাসেট। এখানেও কতকটা সেই আঁচড় কাটার মতই ব্যাপার, তবে আঁচড়টা হত magnetic, ফলে রেকর্ডের মত অত সহজে নষ্ট হত না। তবে সময়ের সাথে সাথে সেই আঁচড়ও ক্রমশঃ ফিকে হয়ে আসত।

এখনকার দিনে আমরা টেপ রেকর্ডার আর ক্যাসেট কমই ব্যবহার করি। তার জায়গা নিয়েছে CD আর DVD. এদের বেলায় শব্দ বা ছবির মান শুধু যে অনেক ভালো তাই নয়, সময়ের সাথে সাথে খারাপও হয় না। বস্তুতঃ প্রথম যখন CD বাজারে আসে, শুনেছি তখন এরকম বিজ্ঞাপন দেওয়া হত যে, CD-র উপর ব্লেড দিয়ে একটা আঁচড় কাটলেও তার রেকর্ডিংয়ের মান কিছুমাত্র নষ্ট হবে না! হাতের কাছে কোনো অদরকারী CD থাকলে পরীক্ষাটা করে দেখতে পারো। CD বা DVD এই আশ্চর্য গুণ কোথা থেকে পায়? এর একটা চট্‌জলদি উত্তর অবশ্য সবাই জানে--ওরা যে digital, তাই! এই "digital" ব্যাপারটা সত্যিই কী? এর মানে হল শব্দ বা ছবি যাই একটা CD বা DVD-র উপর রেকর্ড করা হয়, সেটাকে প্রথমে সংখ্যায় পরিণত করা হয়, এবং সংখ্যাগুলোকে CD বা DVD-র গায় খোদাই করে দেওয়া হয়। সংখ্যা মানেই অংক। CD বা DVD-র সাফল্যের চাবীকাঠিটা আসলে এই অংকের মধ্যেই লুকিয়ে আছে।

এই যে সংখ্যার কথা বললাম, সেটা কিন্তু আমরা যেসব সংখ্যা ব্যবহার করি (যেমন $1, 2, 3, 4$ বা ভগ্নাংশ বা $\sqrt{2}$) এরকম নয়। এগুলো অদ্ভুত নতুন ধরণের সংখ্যা। এদের এমনভাবে সাজানো যায় যে যদি মাঝের থেকে কয়েকটা সংখ্যা মুছে বা বদলেও যায়, তবে বাকি সংখ্যাগুলো থেকে অংক কষে ওদের অনায়াসে পুনরুদ্ধার করা যাবে। একটা CD বা DVD player বস্তুতঃ ক্রমাগত এই অংকটাই করতে থাকে। ফলে, অনেকগুলো সংখ্যা নষ্ট হয়ে গেলেও বাকি সংখ্যাগুলোর থেকেই সবকিছু উদ্ধার করা যায়, তাই তোমার মনে হয় যেন CD বা DVD-টা নতুনের মতই আছে। প্রশ্ন হল এই নতুন সংখ্যাগুলো কী এবং কোথা থেকে আসে? এদের জন্ম হল abstract algebra থেকে। এবং এই কাজে প্রধান দুটো abstract structure হল **ring** এবং তার বড় ভাই **field.** এদের কথাই আমরা এবার শিখব।

প্রথমে শিখব ring-এর কথা। Group-এর সময়ে কাজ করেছিলাম একটা nonempty set আর তার উপর একটা binary operation নিয়ে। এখানেও আমরা কাজ করব একটা nonempty set নিয়ে, কিন্তু তার উপর দুটো binary operation থাকবে। তাদের একটাকে বলব addition (যোগ) আর অন্যটাকে বলব multiplication (গুণ)। হয়তো আন্দাজ করতে পারছ যে, এরা আমাদের ছোটোবেলায় শেখা integer-দের যোগ এবং গুণের আদলে তৈরী--

DEFINITION: Ring

We say $(R, +, \bullet)$ is a **ring** to mean that R is a nonempty set, and $+$ and $\bullet$ are two binary operations on R such that

1. $(R, +)$ is an Abelian group,
2. R is closed under $\bullet$,
3. $\bullet$ is associative,
4. $\bullet$ distributes over $+$, ie,

$$\forall a, b, c \in R \quad a \bullet (b + c) = a \bullet b + a \bullet c$$

and

$$\forall a, b, c \in R \quad (b + c) \bullet a = b \bullet a + c \bullet a.$$

The identity of $(R, +)$ is denoted by 0 and the additive inverse of any element $a \in R$ is denoted by $-a$.

এইখানে গুটিকয়েক কথা বলে রাখা ভালো--

- যখনই বলেছি যে $\bullet$ হল R-এর উপরে একটা binary operation, তার মধ্যেই কিন্তু ধরা আছে যে "R is closed under $\bullet$." সুতরাং ওটাকে আর আলাদা করে লেখার দরকার ছিল না। কিন্তু কোনো কোনো প্রাচীনপন্থী মাষ্টারমশায় closure property-টাকে আলাদা করে না দেখলে বিচলিত হয়ে পড়েন। তাই অনাবশ্যক হলেও ওটাকে আলাদা করে লিখেছি। আধুনিক standard বইতে সাধারণতঃ এটা আলাদা করে লেখে না।
- ওই যে বলেছি $(R, +)$ একটা Abelian group, ওর মধ্যে কিন্তু পাঁচটা শর্ত ঘাপটি মেরে লুকিয়ে আছে--
  1. R is closed under $+$.
  2. $+$ হল associative.
  3. R-এর মধ্যে $+$-এর identity (অর্থাৎ 0) আছে।
  4. প্রত্যেকটা element-এর additive inverse (অর্থাৎ negative) R-এর মধ্যে আছে।
  5. $+$ হল commutative.

লক্ষ কর, যোগের উপর শর্ত বেশী, গুণের উপর শর্ত কম--

- যোগের বেলায় identity থাকতেই হবে, গুণের বেলায় তা না থাকলেও আপত্তি নেই।
- যোগের বেলায় সব element-এর inverse (বা যাকে বলে additive inverse বা negative) থাকতে হবে। গুণের বেলায় identity থাকবে কিনা তারই ঠিক নেই, তো আর inverse[1]!
- যোগটাকে commutative হতেই হবে, কিন্তু গুণটার উপর সেরকম কোনো শর্ত নেই।

[1]কোনো binary operation-এর যদি identity element-ই না থাকে, তবে সেই operation-এর জন্য কোনো element-এর inverse থাকার প্রশ্নই ওঠে না।

Example 1: যেহেতু integer-দের যোগ আর গুণের আদলেই ring-এর সংজ্ঞাটা তৈরী, তাই বলাই বাহুল্য যে, $(\mathbb{Z}, +, \times)$ অবশ্যই একটা ring হবে। ■

Multiplication-এর উপর আমরা কম শর্ত চাপাচ্ছি মানে এই নয় যে, multiplication-টাকে সব সময়ে বিচ্ছিরি কিছু হতে হবে। চাইলে multiplication-টাও নানারকম বাড়তি শর্ত মেনে চলতে পারে, তাতেও আমাদের কোনো আপত্তি নেই। যেমন যদি multiplication-টাও commutative হয়, তবে আমরা খুশীই হব, কারণ সেক্ষেত্রে ring-এর দুটো binary operation-ই commutative হবে (addition তো যে কোনো ring-এর ক্ষেত্রেই commutative). এরকম ring-কে আমরা ভালোবেসে বলি **commutative ring.**

> DEFINITION: **Commutative ring**
>
> A ring $(R, +, \bullet)$ is called **commutative** if $\bullet$ is a commutative operation on R, *i.e.*,
>
> $$\forall a, b \in R \quad a \bullet b = b \bullet a.$$

যদি $(R, +, \bullet)$ একটা ring হয় তবে $\bullet$-এর জন্য কোনো identity element নাও থাকতে পারে। কিন্তু যদি থাকে, তবে আমরা তাকে আদর করে **unity** বলে ডাকি। হাতে সময় থাকলে অবশ্য অনেক সময়ে ওকে **multiplicative identity**-ও বলি। আর লেখার সময়ে সাধারণতঃ লিখি 1.
যদি একটা ring-এ যদি unity থাকে অমনি জানতে ইচ্ছা করে যে কোনো element-এর **multiplicative inverse** আছে কি না। যদি $a \in R$ হয়, তবে তার multiplicative inverse বলতে বোঝাচ্ছি এমন কোনো $b \in R$ যাতে $a \bullet b = b \bullet a = 1$ হয়। এখানে 1 হল ring-এর unity-টা। একটু চিন্তা করলেই বুঝবে যে, অন্ততঃ একটা element আছে যার multiplicative inverse থাকতে বাধ্য, সে হল 1 নিজে। ওর multiplicative inverse-ও 1. কিন্তু বাকিদের বেলায়? এক কথায় কিছু বলা যায় না। Multiplicative inverse থাকতেও পারে, নাও পারে। যাদের multiplicative inverse থাকে তারা আমাদের বিশেষ প্রিয়, এদের ডাকনাম হল **unit.**
এবং এইখানেই প্রচুর ছাত্রছাত্রীর সমস্যা--

7.1.1 Unity আর unit-এর মধ্যে পার্থক্য কী?

একটা উদাহরণ নিয়ে বোঝা যাক। $(\mathbb{Z}, +, \times)$ একটা ring. এর মধ্যে 1 হল unity, কারণ 1 হল একমাত্র সংখ্যা যাকে দিয়ে কোনো কিছু গুণ করলে সেই সংখ্যাটা বদলায় না। এছাড়া আর কোনো unity নেই। (unity কখনোই কোনো ring-এ একাধিক থাকে না।) এবার দেখি unit কটা আছে। Unit বার করার জন্য দেখতে হবে এমন কী কী $m, n \in \mathbb{Z}$ আছে, যাতে $m \times n = 1$ হয়। একটু চিন্তা করলেই দেখবে যে $m = n = 1$ আর $m = n = -1$ নেওয়া ছাড়া কোনো পথ নেই। সুতরাং $\mathbb{Z}$-এর মধ্যে unit আছে ঠিক দুটো, 1 এবং -1.
এই প্রসঙ্গে লক্ষ কর যে--

- একটা ring-এর যদি unity না থাকে, তবে unit থাকার প্রশ্নই নেই।
- যদি কোনো ring-এ unity থাকে, তবে ঠিক একটাই unity থাকবে। কিন্তু unit একাধিকও থাকতে পারে।

Unity আর unit-এর পার্থক্য নিয়ে উপরের আলোচনাটুকু ভালো করে পড়ে নাও। তারপর দ্যাখো নীচের প্রশ্নটার উত্তর দিতে পারো কিনা।

Exercise 1: তিনটে বাক্য দিচ্ছি, এদের মধ্যে কে বা কারা ঠিক বা ভুল বল--

1. এমন ring সম্ভব যাতে unity আছে, কিন্তু একটাও unit নেই।

2. Unity সব সময়েই একটা unit.
3. Unit-রা সব সময়েই unity হয়।

■

7.2 নানারকম ring

অংকের জগতে সবচেয়ে গুরুত্বপূর্ণ ring নিঃসন্দেহে $(\mathbb{R}, +, \times)$, অর্থাৎ real number-দের ring, যেখানে $+$ হল যোগ আর $\times$ হল গুণ। এটা এতই গুরুত্বপূর্ণ একটা ring যে, এর আলাদা করে প্রমাণের দরকার হয় না, এটা $\mathbb{R}$-এর সংজ্ঞার মধ্যেই ধরা আছে। এর পরেই গুরুত্বপূর্ণ হল $\mathbb{Z}$ (মানে integer বা পূর্ণসংখ্যাদের ring) এবং $\mathbb{Q}$ (মানে rational সংখ্যাদের ring). আরেকধরণের দরকারী ring হল matrix-দের ring. সেটা এইরকম--ধরো R কোনো একটা ring, আর n কোনো একটা positive integer. তাহলে $M_n(R)$ মানে হল সেই সব $n \times n$ matrix-দের set যাদের প্রতিটা entry হল R-এর সদস্য। যেমন এই নীচের matrix-টা $M_2(\mathbb{R})$-এর সদস্য--

$$\begin{bmatrix} 1 & \frac{1}{2} \\ 2 & 4 \end{bmatrix}$$

কিন্তু এটা $M_2(\mathbb{Z})$-এর মধ্যে নেই, কারণ $\frac{1}{2} \notin \mathbb{Z}$. যে কোনো R-এর জন্যই $M_n(R)$ একটা ring হয়, যেখানে binary operation দুটো হল matrix-এর যোগ আর গুণ।
এবার আমরা কিছু অংক করব যেখানে একটা set আর দুটো binary operation দিয়ে ring হয় কিনা দেখাতে বলবে।

Example 2: Let S denote the set of all functions $f : \mathbb{R} \to \mathbb{R}$. Define '+' and '*' on S by

$$(f + g)(a) = f(a) + g(a) \text{ and } (f * g)(a) = f(a)g(a)$$

for all $a \in \mathbb{R}$ and for all $f, g \in S$. Assuming S to be an additive Abelian group, show that $(S, +, *)$ is a commutative ring with identity. **(2001)**
SOLUTION: আগেই বলেছি যে commutative ring with identity দেখানো বেশ লম্বা কাজ, অনেকগুলো শর্ত পরীক্ষা করে দেখতে হবে। কিন্তু এই অংকটায় আমাদের কাজ কমিয়ে দিয়েছে এই বলে যে, S-কে additive Abelian group বলে ধরে নেওয়া যেতে পারে। সুতরাং প্রথম অনেকগুলো ধাপ আর কষতে হবে না। এখন খালি পাঁচটা কাজ পড়ে আছে--

> Since S is already assumed to be a group, enough to show that
>
> 1. S is closed under $*$,
> 2. $*$ is associative,
> 3. $*$ distributes over $+$,
> 4. $*$ is commutative,
> 5. $*$ has identity in S.

এর মধ্যে প্রথম তিনটের জন্য S একটা ring, আর বাকী দুটো দরকার কারণ ring-টাকে commutative with identity দেখাতে বলা হয়েছে। এখানে identity মানে multiplicative identity বা unity.

Step 1: S is closed under $*$: If $f, g \in S$ then $\forall x \in \mathbb{R}$ $f(x), g(x) \in \mathbb{R}$,
and so $(f * g)(x) = f(x)g(x) \in \mathbb{R}$.
So $f * g$ is a function from $\mathbb{R}$ to $\mathbb{R}$. $\therefore f * g \in S$, as required.

Step 2: $*$ is associative: To show

$$\forall f, g, h \in S \quad (f * g) * h = f * (g * h).$$

$\forall f, g, h$ Take any $f, g, h \in S$.

এখানে $(f * g) * h$ এবং $f * (g * h)$ দুজনেই $\mathbb{R}$ থেকে $\mathbb{R}$-এ function. সুতরাং এদের সমান দেখানো মানে এটা দেখানো যে, সব $x \in \mathbb{R}$-এই এদের value সমান।

Then, for every $x \in \mathbb{R}$,

$$\begin{aligned} ((f * g) * h)(x) &= (f * g)(x)h(x) \\ &= (f(x)g(x))h(x) \\ &= f(x)(g(x)h(x)) \quad [\because \text{ multiplication in } \mathbb{R} \text{ is associative}] \\ &= f(x)(g * h)(x) \\ &= (f * (g * h))(x). \end{aligned}$$

So $(f * g) * h = f * (g * h)$, as required.

এর পর আমাদের distributive দেখানোর কথা, কিন্তু তার আগে commutative দেখিয়ে নিলে সুবিধা হবে। কারণ তাহলে distributive দেখানোর সময়ে খালি $f * (g + h) = f * g + f * h$ দেখালেই চলবে, আলাদা করে আর $(g + h) * f = g * f + h * f$ দেখাতে হবে না।

Step 3: $*$ is commutative:

To show:

$$\forall f, g \in S \quad f * g = g * f.$$

$\forall f, g$ Take any $f, g \in S$.

Then, for every $x \in \mathbb{R}$,

$$(f * g)(x) = f(x)g(x) = g(x)f(x) = (g * f)(x),$$

since multiplication in $\mathbb{R}$ is commutative.

Step 4: $*$ distributes over $+$:

To show that

$$\forall f, g, h \in S \quad f * (g + h) = f * g + f * h \quad \text{and} \quad (g + h) * f = g * f + h * f.$$

$\forall f, g, h$ Take any $f, g, h \in S$.

Then, for every $x \in \mathbb{R}$,

$$\begin{aligned}(f*(g+h))(x) &= f(x)(g+h)(x) \\ &= f(x)(g(x)+h(x)) \\ &= f(x)g(x)+f(x)h(x) \\ &\quad \because \text{multiplication distributes over addition in } \mathbb{R} \\ &= (f*g+f*h)(x).\end{aligned}$$

So $f*(g+h) = f*g+f*h$, as required.

By commutativity, $(g+h)*f = g*f+h*f$, as required.

Step 5: $*$ has identity: The constant function $i(x) \equiv 1$ is the identity because $\forall f \in S \quad \forall x \in \mathbb{R}$

$$(f*i)(x) = f(x)i(x) = f(x) \times 1 = f(x),$$

So, by commutativity, we have $f*i = i*f = f$.

■

Example 3: If $\mathbb{C}$ denotes the set of complex numbers, show that the additive Abelian group $(\mathbb{C},+)$ forms a ring $(\mathbb{C},+,\bullet)$ under the usual addition and multiplication. **(2004)**

SOLUTION: এখানে যা প্রমাণ করতে হবে, সেগুলো সবই আমরা হায়ার সেকণ্ডারী থেকেই জানি, খালি খুঁটিয়ে খুঁটিয়ে লিখতে হবে।

Since $(\mathbb{C},+)$ is already given to be an Abelian group, it is enough to show the following properties:

Step 1: $\mathbb{C}$ is closed under $\bullet$: To show

$\forall w,z \in \mathbb{C} w \bullet z \in \mathbb{C}$.

$\forall w, z$ Take any $w, z \in \mathbb{C}$.

Then $w = a + \mathbf{i}b$ and $z = c + \mathbf{i}d$ for some $a,b,c,d \in \mathbb{R}$.

$$\therefore wz = (a+\mathbf{i}b) \bullet (c+\mathbf{i}d) = (ac-bd) + \mathbf{i}(ad+bc) \in \mathbb{C},$$

since $ac-bd, ad+bc \in \mathbb{R}$. So $\mathbb{C}$ is closed under multiplication.

Step 2: $\bullet$ is associative: To show

$\forall v,w,z \in \mathbb{C} (v \bullet w) \bullet z = v \bullet (w \bullet z)$.

$\forall v, w, z$ Take any

$$v = a + \mathbf{i}b, \quad w = c + \mathbf{i}d, \quad z = e + \mathbf{i}f, (a, ..., f \in \mathbb{R}).$$

Then

$$\begin{aligned}(vw)\bullet z &= ((a+\mathbf{i}b)\bullet(c+\mathbf{i}d))\bullet(e+\mathbf{i}f)\\ &= (ac-bd+\mathbf{i}(bc+ad))\bullet(e+\mathbf{i}f)\\ &= (ace-bde-bcf-adf)+\mathbf{i}(acf-bdf+bce+ade).\end{aligned}$$

Similarly,

$$\begin{aligned}v\bullet(w\bullet z) &= (a+\mathbf{i}b)\bullet((c+\mathbf{i}d)\bullet(e+\mathbf{i}f))\\ &= (a+\mathbf{i}b)\bullet(ce-df+\mathbf{i}(cf+de))\\ &= (ace-bde-bcf-adf)+\mathbf{i}(acf-bdf+bce+ade),\end{aligned}$$

which is the same as $(v\bullet w)\bullet z$, as required.

Step 3: Distribution law: To show

$\forall w,x,z\in\mathbb{C} w\bullet(x+z)=w\bullet x+w\bullet z$ and $(x+z)\bullet w=x\bullet w+z\bullet w$.

$\forall w,x,z$ Take any $w,x,z\in\mathbb{C}$.

Then $w=a+\mathbf{i}b, x=c+\mathbf{i}d$ and $z=p+\mathbf{i}q$, for some $a,b,c,d,p,q\in\mathbb{R}$.

So

$$w\bullet(x+z) = (a+\mathbf{i}b)\bullet((c+p)+\mathbf{i}(d+q))$$

Again,

$$\begin{aligned}&w\bullet x+w\bullet z\\ =\;& (a+\mathbf{i}b)\bullet(c+\mathbf{i}d)+(a+\mathbf{i}b)\bullet(p+\mathbf{i}q)\\ =\;& [(ac-bd)+\mathbf{i}(ad+bc)]+[(ap-bq)+\mathbf{i}(aq+bp)]\\ =\;& [ac+ap-bd-bq]+\mathbf{i}[ad+aq+bc+bp],\end{aligned}$$

which is the same as $w\bullet(x+z)$ as required.

Similar argument shows that $(x+z)\bullet w=x\bullet w+z\bullet w$.

■

7.3 একটা অদ্ভুত প্রয়োগ

আমরা গোড়ার দিকে CD আর DVD-র কথা উল্লেখ করেছিলাম। সেখানে বলেছিলাম, ring ব্যবহার করে নানারকম নতুন নতুন সংখ্যা বানানো যায়। একটা ছোট্টো উদাহরণ দেখি। এই আলোচনাটুকু খালি মজা পাবার জন্য। যারা কেবল পরীক্ষা পাশের জন্য এই বইটা পড়ছ (এবং মজা-টজা যারা একটুও ভালোবাসো না) তারা স্বচ্ছন্দে আজকের বাকি অংশটুকু বাদ দিয়ে যেতে পারো।

দুনিয়ায় যতরকম ring আছে, তার মধ্যে অন্যতম গুরুত্বপূর্ণ হল **polynomial ring.** কাকে polynomial বলে মনে

$$\begin{array}{r|l} & 3 \\ x^2+1 & 3x^2+4x+2 \\ & 3x^2 \qquad\quad +3 \\ \hline & \qquad\quad 4x-1 \end{array}$$

Fig 1

$$\begin{array}{r|l} & bd \\ x^2+1 & bdx^2+(ad+bc)x+ac \\ & bdx^2 \qquad\qquad\qquad +bd \\ \hline & \qquad (ad+bc)x+(ac-bd) \end{array}$$

Fig 2

আছে নিশ্চয়ই--

$$1-2x+3x^2, \quad e+\pi x^3, \quad 24x-\tfrac{3}{4}x^{10}, \text{ ইত্যাদি।}$$

অর্থাৎ এইরকম চেহারার যেকোনো জিনিস--

$$a_0+a_1x+\cdots+a_nx^n,$$

যেখানে $n \geq 0$ হল একটা integer, আর $a_0,...,a_n$-দের বলে একেকটা **coefficient.** এখানে coefficient-গুলোকে সব real number নিয়েছি (মানে $a_0,...,a_n \in \mathbb{R}$), তাই এটাকে বলব একটা real polynomial. দুটো polynomial-কে কী করে যোগ আর গুণ করতে হয় সে তো আমরা স্কুলে থাকতেই শিখেছি, যেমন

$$(1+3x)+(1-4x)=2-x \text{ আর } (1+3x)(1-4x)=1-x-12x^2.$$

একটু চিন্তা করলেই বুঝবে যে, এই যোগ আর গুণ যাবতীয় real polynomial-রা একটা ring করে। এই অব্ধি তেমন নতুন কিছু নেই। এবার মজাটা। আমরা একটা অদ্ভুত কাণ্ড করব। কায়দাটা খুবই সহজ, যদিও এটা প্রথমে ভেবে বার করতে পণ্ডিতদের অনেক মাথা ঘামাতে হয়েছিল। আমরা এই polynomial-টা নেব: $1+x^2$, এবং এটা দিয়ে সব polynomial-কে ভাগ করে ভাগশেষ বার করব। যেমন ধরো $3x^2+4x+2$-কে $1+x^2$ দিয়ে ভাগ করলে ভাগশেষ থাকে $4x-1$. ভাগটা করে দেখিয়েছি Fig 1-এ। বুঝতেই পারছ এইভাবে যদি সব polynomial-কেই ছেঁটে দিতে থাকি, তবে যে ভাগশেষগুলো পড়ে থাকবে তারা সবাই হবে হয় constant polynomial, আর নয় তো degree 1-ওয়ালা polynomial. কারণ x^2+1-এর degree-ই হল 2, অতএব ভাগশেষদের degree কোনোভাবেই ≥ 2 হতে পারে না। এইবার দেখি এইভাবে ভাগশেষ নেওয়ার ফলে যোগ এবং গুণের কী দশা হয়েছে। ধরো দুটো ভাগশেষ নিলাম--

$$a+bx \text{ আর } c+dx.$$

এদের যদি গুণ করি, তবে হওয়ার কথা ছিল

$$(a+bx)(c+dx)=ac+(ad+bc)x+bdx^2.$$

কিন্তু ভাগশেষ নেওয়ার দৌরাত্মে কোনো x^2-এর তো টিঁকে থাকার জো নেই। সুতরাং $1+x^2$ দিয়ে এই গুণফলটাকে ভাগ করলে (Fig 2) ভাগশেষ পেলাম $(ac-bd)+(ad+bc)x$. সুতরাং গুণের নিয়মটা দাঁড়ালো

$$(a+bx)(c+dx)=(ac-bd)+(ad+bc)x. \qquad (*)$$

অবশ্য যোগের ক্ষেত্রে কোনোভাবে x^2 এসে পড়ার সম্ভাবনা নেই, তাই যোগের ক্ষেত্রে আমাদের পরিচিত নিয়মটাই বহাল থাকবে--

$$(a+bx)+(c+dx)=(a+c)+(b+d)x. \qquad (**)$$

সুতরাং আমরা একধরণের নতুন সংখ্যার জগতে এসে উপস্থিত হলাম--যাদের দেখতে $a+bx$-এর মত এবং যাদের যোগ আর গুণ করা যায় (**) এবং (*)-এর মত করে।

তুমি হয়তো মুখ বাঁকিয়ে বলবে--এ মা, এ আবার কী রকম সংখ্যা হল, আর এসব করে লাভই বা কী হল? উত্তরে আমি বলব--ভালো করে তাকিয়ে দ্যাখো, ওরা তোমার খুবই চেনা জিনিস, এবং অংকের জগতে ওদের গুরুত্বও অপরিসীম, ওরাই

আসলে complex number. আমরা এখানে ওদের $a+bx$ আকারে লিখেছি বলে হয়তো চিনতে অসুবিধা হচ্ছে, ওই x-এর বদলে $|ii$ কল্পনা করে নাও, অমনি ওদের $a+\mathbf{i}b$ বলে চিনতে পারবে। আর (*)-এ যে গুণের নিয়মটা দেওয়া হয়েছে, সেটাও আসলে complex number-এর গুণেরই সংজ্ঞা!
ঠিক এই পথেই complex number-দের জন্ম। শুধু complex number-ই নয়, আরও বহু ধরণের সংখ্যারই সৃষ্টি করা যায় এইভাবে--প্রথমে একটা polynomial ring নিতে হয়, তার পর তা থেকে একটা বিশেষ polynomial নিতে হয় (যেমন আমরা $1+x^2$ নিয়েছিলাম)। এই polynomial-টার খালি একটা বৈশিষ্ট্য থাকতে হবে, যেন factorise (মানে উৎপাদকে বিশ্লেষণ) না করা যায়। তারপর সেটা দিয়ে সব polynomial-কে ভাগ করে ভাগশেষ নিলেই এরকম নতুন নতুন সংখ্যা পাওয়া যায়! CD আর DVD-র জন্য যে সব সংখ্যা লাগে সেগুলোও সবই এই একই কায়দায় পাওয়া। আমরা এই বইতে আর এ বিষয়ে আলোচনা করব না। কিন্তু এই রকম কায়দায় নতুন নতুন সংখ্যা বানানো এবং তাদের গুণাগুণ বিচার করা নিয়ে অংকের একটা আস্ত শাখাই আছে, তার নাম Galois theory (গ্যালোয়া থিওরী)।

DAY 8
Ring (part 2)

8.1 Subring

Group-এর ক্ষেত্রে যেমন subgroup, তেমনি ring-এর বেলায় হল **subring.** সংজ্ঞাটা এইরকম--

> DEFINITION: **Subring**
>
> Let $(R,+,\bullet)$ be a ring. Then $S\subseteq R$ is called a **subring** if $(S,+,\bullet)$ is again a ring.

এইবারের অংকগুলোতে আমাদের একটা করে ring আর তার একটা subset দেওয়া থাকবে। আমাদের কাজ হবে subset-টা একটা subring কিনা পরীক্ষা করে দেখা।
একটা set-কে ring দেখানোর চেয়ে, একটা ring-এর subset-কে subring দেখানো সাধারণতঃ অনেক সোজা। কারণ মূল ring থেকে অনেক কিছুই সরাসরি পাওয়া যায় (যেমন associativity, distributivity), সেগুলো আর নতুন করে প্রমাণ করতে হয় না।
একটা ring-এর কোনো subset-কে একটা subring দেখানোর জন্য তিনটে জিনিস দেখালেই চলে--

1. subset-টা nonempty,
2. subset-টা closed under difference, অর্থাৎ subset-এর দুটো element নিয়ে একটা থেকে অন্যটা বিয়োগ করলে বিয়োগফলটা subset-এর ভিতরেই থাকে,
3. subset-টা closed under multiplication, অর্থাৎ subset-এর দুটো element নিয়ে গুণ করলে গুণফলটা subset-এর ভিতরেই থাকে।

Example 4: True or false? Justify. The set

$$S=\left\{\begin{bmatrix} a & b\\ c & d\end{bmatrix}\in M_2(\mathbb{R})\ \Big|\ a+c=b+d\right\}$$

is a subring of the ring $M_2(\mathbb{R})$ of all 2×2 real matrices. **(1998,2006)**
SOLUTION: প্রথমেই লিখে নেওয়া ভালো আমরা ঠিক প্রমাণ করব নাকি ভুল দেখাব। এখানে আমরা ঠিকের পক্ষে।

> The result is true.

এই কথাটা আমরা কী করে গোড়াতেই জানলাম? এর উত্তর হচ্ছে, গোড়াতে আমরা মোটেই এটা জানতাম না। নীচের অংশটা শেষ করে তবে ওই প্রথম লাইনটা লিখেছি। গোড়াতে যেটুকু জানতাম তা হল এই যে, S-কে subring দেখাতে হলে তিনটে জিনিস দেখাতে হবে-- প্রথমতঃ $S \neq \phi$. দ্বিতীয়তঃ, S closed under difference, আর তৃতীয়তঃ, S-কে closed under multiplication হতে হবে।
আমাদের প্রথম কর্তব্য রাফে কষে দেখা যে, এই তিনটে শর্তই আমাদের S পালন করে কিনা। যদি অন্ততঃ একটা শর্তও পালিত না হয়, তবে উত্তরে কেবলমাত্র সেই কথাটাই গুছিয়ে লিখে সিদ্ধান্ত করব যে, S একটা subring নয়। কিন্তু যদি তিনটেই পালিত হয়, তবে তিনটেরই প্রমাণ দিতে হবে। আমাদের ক্ষেত্রে তিনটেই পালিত হয়েছে।
প্রথমে দেখাব $S \neq \phi$. তার জন্য S-এর ভিতরে কিছু একটা আছে দেখালেই চলবে।

> Step 1: Nonempty: Clearly $S \neq \phi$, since taking $a = b = c = d = 0$,
>
> $$\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \in S.$$

এরপরের কাজ closed under difference দেখানো। এর জন্য S-এর মধ্যে যেকোনো দুটো matrix নেব, এবং একটা থেকে অন্যটাকে বিয়োগ করে দেখাব যে বিয়োগফলটাও S-এর মধ্যেই আছে।

> Step 2: Closure under difference: Let
>
> $$\begin{aligned} & \begin{bmatrix} a & b \\ c & d \end{bmatrix}, \begin{bmatrix} p & q \\ r & s \end{bmatrix} \in S \\ \therefore \quad & a+c = b+d \quad \& \quad p+r = q+s \\ \therefore \quad & (a-p)+(c-r) = (b-q)+(d-s) \\ \therefore \quad & \begin{bmatrix} a & b \\ c & d \end{bmatrix} - \begin{bmatrix} p & q \\ r & s \end{bmatrix} = \begin{bmatrix} a-p & b-q \\ c-r & d-s \end{bmatrix} \in S. \end{aligned}$$

শেষ ধাপটাও আগেরই মত, খালি এবার বিয়োগফলের বদলে গুণফল নিয়ে কাজ করব।

> Step 3: Closure under multiplication: Let
>
> $$\begin{bmatrix} a & b \\ c & d \end{bmatrix}, \begin{bmatrix} p & q \\ r & s \end{bmatrix} \in S.$$
>
> Then
>
> $$a+c = b+d \text{ and } p+r = q+s$$
>
> Now,
> $$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} p & q \\ r & s \end{bmatrix} = \begin{bmatrix} ap+br & aq+bs \\ cp+dr & cq+ds \end{bmatrix}.$$
>
> We shall show that
>
> $$(ap+br)+(cp+dr) = (aq+bs)+(cq+ds).$$
>
> Here $LHS = p(a+c)+r(b+d) = (a+c)(p+r)$, since $a+c = b+d$.

> Similarly,
>
> $$\begin{aligned} RHS &= q(a+c)+s(b+d) \\ &= (a+c)(q+s) \quad [\because a+c=b+d] \\ &= (a+c)(p+r) = LHS, \end{aligned}$$
>
> Since $q+s=p+r$.

খালি এই তিনটে শর্ত দেখালেই যে চলছে তার কারণ বাকী শর্তগুলো সব মূল ring (অর্থাৎ এক্ষেত্রে $M_2(\mathbb{R})$) থেকেই পাওয়া যাচ্ছে। এই কথাটা এখানে উল্লেখ করে দেওয়া ভালো।

> All other properties are inherited from $M_2(\mathbb{R})$.

এখানে ইংরাজীটা লক্ষ কর-- "inherited" মানে উত্তরাধিকারসূত্রে পাওয়া। এই ভাষাটা আমরা দ্বিতীয় অধ্যায়ে subgroup-এর ক্ষেত্রেও ব্যবহার করেছিলাম। ■

Example 5: Show that the set of matrices

$$\begin{bmatrix} p & q \\ 0 & r \end{bmatrix}$$

is a subring of the ring of 2×2 matrices with integral elements, the operations being matrix addition and matrix multiplication.[3] **(2008)**

SOLUTION: এখানে "matrices with integral elements" মানে হল এমন সব matrix, যাদের প্রতিটা সংখ্যাই একেকটা integer.

> Let $M_2(\mathbb{Z})$ be the ring of 2×2 matrices with integral elements.
>
> Let the given set be R.
>
> Nonempty: Taking $p, q, r = 0$,
>
> $$\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \in R.$$
>
> Closed under difference and multiplication: If
>
> $$\begin{bmatrix} p_1 & q_1 \\ 0 & r_1 \end{bmatrix}, \begin{bmatrix} p_2 & q_2 \\ 0 & r_2 \end{bmatrix} \in R,$$
>
> then $p_i, q_i, r_i \in \mathbb{Z}$ for $i = 1, 2$. So
>
> $$\begin{bmatrix} p_1 & q_1 \\ 0 & r_1 \end{bmatrix} - \begin{bmatrix} p_2 & q_2 \\ 0 & r_2 \end{bmatrix} = \begin{bmatrix} p_1 - p_2 & q_1 - q_2 \\ 0 & r_1 - r_2 \end{bmatrix} \in R,$$
>
> Since $p_1 - p_2, q_1 - q_2, r_1 - r_2 \in \mathbb{Z}$.

Also

$$\begin{bmatrix} p_1 & q_1 \\ 0 & r_1 \end{bmatrix} \begin{bmatrix} p_2 & q_2 \\ 0 & r_2 \end{bmatrix} = \begin{bmatrix} p_1p_2 & p_1q_2 + q_1r_2 \\ 0 & r_1r_2 \end{bmatrix} \in R,$$

since $p_1p_2, p_1q_2 + q_1r_2, r_1r_2 \in \mathbb{Z}$.

All other properties are inherited from $M_2(\mathbb{Z})$.

Hence R is a subring of $M_2(\mathbb{Z})$, as required.

■

Example 6: True or false? Justify. If R is a ring and a is a fixed element of R then the set $S = \{x \in R : xa = 0\}$ is a subring of R. **(2002)**

SOLUTION:

The statement is true.

Step 1: Nonempty: Clearly $S \neq \phi$, since $0 = 0a \in S$.

Step 2: Closure under difference:

Take any $x, y \in S$. Then

$$\begin{aligned} & xa = ya = 0 \\ \implies & (x-y)a = 0 \\ \implies & x - y \in S. \end{aligned}$$

Step 3: Closure under multiplication:

Take any $x, y \in S$. Then

$$\begin{aligned} & xa = ya = 0 \\ \implies & (xy)a = x(ya) = x0 = 0 \\ \implies & xy \in S. \end{aligned}$$

All other properties are inherited from R.

■

Example 7: Let R be a ring and a be a fixed element of R. Then prove that the set

$$S = \{x \in R \mid x \cdot a = 0\}$$

is a subring of R.[2] **(2012.5a)**

SOLUTION: আগের অংকটাই। ■

Example 8: Let a be a fixed element of a ring R. Let

$$C(a) = \{x \in R \ : \ xa = ax\}.$$

Prove that $C(a)$ is a subring of R.[2] **(2010.5ai)**

SOLUTION:

Nonempty: If we take $x = a$ then

$$xa = a^2 = ax.$$

So $a \in C(a)$. Hence $C(a) \neq \phi$.

Closed under subtraction: Shall show

$$\forall x, y \in C(a) \quad x - y \in C(a).$$

$\forall x, y$ Take any $x, y \in C(a)$.

Then $ax = xa$ and $ay = ya$.

So

$$\begin{aligned} a(x-y) &= ax - ay && [\text{ by distributivity}] \\ &= xa - ya && [\text{ property of } a] \\ &= (x-y)a && [\text{ by distributivity}] \end{aligned}$$

$\therefore x - y \in C(a)$, as required.

Closed under multiplication: Shall show

$$\forall x, y \in C(a) \quad xy \in C(a).$$

$\forall x, y$ Take any $x, y \in C(a)$.

Then $ax = xa$ and $ay = ya$.

So

$$\begin{aligned} a(xy) &= (ax)y && [\text{ by associativity}] \\ &= (xa)y && [\text{ property of } a] \\ &= x(ay) && [\text{ by associativity}] \\ &= x(ya) && [\text{ property of } a] \\ &= (xy)a && [\text{ by associativity}] \end{aligned}$$

$\therefore xy \in C(a)$, as required.

Hence $C(a)$ is a subring.

■

8.2 Subring-এর unity

Group-এর বেলায় আমরা দেখেছিলাম যে group-এর identity আর subgroup-এর identity সর্বদা একই হয়। কিন্তু ring-এর বেলায় ঘটনা অন্যরকম। ধরো R একটা ring, আর S তার একটা subring. তাহলে এই পাঁচটা ব্যাপারই সম্ভব--

1. R এবং S দুজনেরই একই unity,
2. R এবং S দুজনেরই unity আছে, কিন্তু unity দুটো আলাদা,
3. R-এর unity আছে, কিন্তু S-এর কোনো unity নেই,
4. R-এর কোনো unity নেই, অথচ S-এর দিব্যি unity আছে,
5. R এবং S কারোরই unity নেই।

এবার এই নিয়ে কয়েকটা অংক করি।

Example 9: Show that the set $T = \{(a, 0) \mid a \in \mathbb{Z}\}$ is a subring of the ring $\mathbb{Z} \times \mathbb{Z}$, where $\mathbb{Z}$ is the ring of integers and the addition and multiplication in $\mathbb{Z} \times \mathbb{Z}$ are defined by

$$(a, b) + (c, d) = (a + c, b + d) \text{ and } (a, b)(c, d) = (ac, bd).$$

Is the identity element of T equal to the identity element of $\mathbb{Z} \times \mathbb{Z}$? Justify. **(2002)**

SOLUTION: প্রথম অংশটা আগের মতই করে ফেলা যাবে।

> Step 1: Nonempty:
>
> $T \neq \phi$ because taking $a = 0 \in \mathbb{Z}$, we have $(0, 0) \in T$.
>
> Step 2: Closure under difference:
>
> $$(a, 0), (b, 0) \in T \implies (a, 0) - (b, 0) = (a - b, 0) \in T,$$
>
> since $a - b \in \mathbb{Z}$.
>
> Step 2: Closure under multiplication:
>
> $$(a, 0), (b, 0) \in T \implies (a, 0)(b, 0) = (ab, 0) \in T,$$
>
> since $ab \in \mathbb{Z}$.

এবার উত্তরাধিকারের কৃতজ্ঞতা স্বীকার করে নিই--

> All other properties are inherited from $\mathbb{Z} \times \mathbb{Z}$.
> Hence T is a subring of $\mathbb{Z} \times \mathbb{Z}$, as required.

এবার unity-র গল্প--

> No, the multiplicative identity of T is different from the multiplicative identity of $\mathbb{Z} \times \mathbb{Z}$.
>
> The identity of T is $(1, 0)$.

⟦ Because:

Take any $(a,0) \in T$. Then

$$(a,0)(1,0) = (a\times 1, 0\times 0) = (a,0) \text{ and } (1,0)(a,0) = (1\times a, 0\times 0) = (a,0).$$

⟧

The identity of $\mathbb{Z}\times\mathbb{Z}$ is $(1,1)$.

⟦ Because:

Take any $(a,b) \in \mathbb{Z}\times\mathbb{Z}$. Then

$$(a,b)(1,1) = (1,1)(a,b) = (a,b).$$

⟧

■

নীচের অংকটাও ring এবং subring-এর multiplicative identity (অর্থাৎ unity) নিয়ে।

Example 10: Give an example of a non-commutative ring without unity having a subring with a different unity.[2] **(2010.4ai)**

SOLUTION: বোধহয় without-এর জায়গায় with বলতে চেয়েছিল, নইলে অংকটার ঠিক মানে হয় না। সুতরাং এখানে এমন একটা ring চেয়েছে যার মধ্যে unity আছে, এবং তার এমন একটা subring চেয়েছে, যার মধ্যেও একটা unity আছে, অথচ ring-এর unity আর subring-এর unity আলাদা। আগের অংকের উদাহরণটা দিলেই চলত, কিন্তু এমন একটা ring চেয়েছে, যেটা আবার non-commutative-ও বটে। আগের অংকের ring-টা ছিল commutative. কিন্তু আমরা ওই আগের অংকের কায়দাতেই এগোব। ওখানে আমাদের ring-টা ছিল $\mathbb{Z}\times\mathbb{Z}$, আর subring-টা ছিল $\mathbb{Z}\times\{0\}$. এবার আমরা $\mathbb{Z}$-এর জায়গায় $M_2(\mathbb{R})$ নেব (মানে যাবতীয় 2×2 সাইজের real matrix-এর ring). আমরা জানি যে সেটা commutative নয়।

Let $R = M_2(\mathbb{R}) \times M_2(\mathbb{R})$, which is a non-commutative ring under the operations

$$(A,B) + (C,D) = (A+C, B+D)$$

and

$$(A,B)(C,D) = (AC, BD).$$

This ring has unity (I,I), where I is identity matrix.

But consider the subring $S = \{(A,O) \ : \ A \in M_2(\mathbb{R})\}$, where O is the zero matrix.

S has unity (I,O), which is different from (I,I).

■

নীচের অংকটা করলে বুঝবে যে ring এবং subring-এর মধ্যে unity-ঘটিত সমস্যা আরও গুরুতর রূপ নিতে পারে। এমন হতেই পারে যে ring-টার unity আছে, অথচ তার কোনো একটা subring-এর মধ্যে কোনোই unity নেই! এরকম একটা উদাহরণ চেয়েছে এবার।

Example 11: Give an example of a subring without unity of a ring with unity.[2] **(2009.5ci)**

SOLUTION:

$(\mathbb{Z}, +, \times)$ is a ring with unity 1.

The set of all even numbers $2\mathbb{Z} = \{2n : n \in \mathbb{Z}\}$ forms a subring. But it has no unity.

⟦ Because:

Let, if possible, $m \in 2\mathbb{Z}$ be the unity.
Then $\forall k \in 2\mathbb{Z} \quad mk = k$.
In particular, for $k = 2$ we must have $2m = 2$. or
$m = 1 (\Rightarrow\Leftarrow \because 1$ is not even, $\therefore m \notin 2\mathbb{Z})$.

⟧

■

Exercise 2: আচ্ছা, এর উল্টোটাও কি হতে পারে? মানে এমন ring কি সম্ভব, যার কোনো unity নেই, অথচ তার একটা subring-এর unity আছে? উত্তরটা খুব কঠিন কিছু নয়, মালমশলা সব আগের অংকটার সমাধানের মধ্যেই আছে। ঠাণ্ডা মাথায় চিন্তা কর। ■

Exercise 3: এমন একটা *non-commutative* ring দিতে পারো যার কোনো unity নেই, অথচ তার একটা subring-এর unity আছে? ■

8.3 Union/intersection

Example 12: True or false? Justify. Union of two proper subrings is a subring. **(2004)**

SOLUTION: এখানে proper শব্দটা অনাবশ্যক।

The result is false. Consider the ring $\mathbb{Z}$ under the usual operations. Then the set $2\mathbb{Z}$ is a subring.

সংক্ষেপে লিখে দেওয়া ভালো আমাদের এই দাবীর কারণ কী--

⟦ Because:

1. Nonempty: $0 \in 2\mathbb{Z}$.
2. Closed under difference:
   $\forall m, n \in \mathbb{Z} \quad 2m - 2n = 2(m - n) \in 2\mathbb{Z}$.
3. Closed under multiplication:
   $\forall m, n \in \mathbb{Z} \quad 2m \times 2n = 2(2mn) \in 2z$.

All other properties are inherited from $\mathbb{Z}$.

>]]
> Similarly, $3\mathbb{Z}$ is a subring.

এখানে আর কারণ ব্যাখ্যা করলাম না, স্রেফ "similarly" লিখে ছেড়ে দিলাম।

> But their union is not a subring, because it is not closed under difference:
> $2 \in 2\mathbb{Z},\ 3 \in 3\mathbb{Z}$,
> $\therefore 2, 3 \in 2\mathbb{Z} \cup 3\mathbb{Z}$.
> But $3 - 2 = 1 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$.

■

Union-এর বেলায় সমস্যা হলেও intersection-এর ক্ষেত্রে কোনো সমস্যা নেই। সেটাই নীচের অংকটার বক্তব্য।

Exercise 4: Prove that the intersection of two subrings must again be a subring. ■

DAY 9
Ring (part 3)

এবার আমরা ring ব্যবহার করে কিছু অংক কষব। প্রথমে খুব সহজ জিনিস দিয়ে শুরু করি।

9.1 সহজ কিছু অংক

Example 13: Let R be a ring. Then prove that

$$\forall a, b \in R \quad a0 = 0a = 0 \text{ and } (-a)(-b) = ab.$$

(1997)
SOLUTION:

> Using properties of a ring we have
>
> $$\begin{aligned} a0 &= a(0+0) \quad [\because 0 = 0+0] \\ &= a0 + a0 \quad [\text{by distribution law}]. \end{aligned}$$
>
> Subtracting $a0$ from both sides we get $0 = a0$, as required.
> Similarly,
>
> $$0a = (0+0)a = 0a + 0a.$$
>
> Subtracting $0a$ from both sides, $0 = 0a$, as required.

এবার দ্বিতীয় অংশ। স্কুলে যদি $(-a)(-b) = ab$ দেখাতে বলত, তবে আমরা দেখাতাম $(-a)(-b) = -(a(-b)) = ab$, অর্থাৎ মাইনাস দুটোকে একে একে ব্র্যাকেটের বাইরে আনতাম, এবং দ্বিতীয় মাইনাসটা বাইরে আসামাত্র প্রথম মাইনাসটার সঙ্গে কাটাকাটি হয়ে যেত।
এখানেও আমরা ঠিক সেই পথেই এগোব। প্রথমে দেখাব $(-a)(-b) = -(a(-b))$, এবং তারপরে দেখাব $-(a(-b)) = ab$. কোনো জিনিসকে আরেকটা জিনিসের negative দেখানোর কায়দা হল ওদের যোগফলটাকে 0 দেখানো। এই কায়দা আমরা বার বার ব্যবহার করব।

$$\begin{aligned} &(-a)(-b) + a(-b) \\ &= (-a + a)(-b) \quad [\text{ distribution law}] \\ &= 0(-b) \\ &= 0, \end{aligned}$$

by part 1 of this problem.
So

$$(-a)(-b) = -(a(-b)). \qquad (\mathbf{A})$$

একই কায়দা আরেকবার--

Now,

$$\begin{aligned} &ab + a(-b) \\ &= a(b + (-b)) \quad [\text{ distribution law}] \\ &= a0 \\ &= 0, \end{aligned}$$

by part 1.
So

$$ab = -(a(-b)). \qquad (\mathbf{B})$$

Hence from (**A**) and (**B**) we have $(-a)(-b) = ab$, as required.

■

Example 14: Let R be a ring. Prove that $a0 = 0a = 0$ for all $a \in R$.[1] **(2010.5bi)**

SOLUTION: আগের অংকের প্রথম অংশটাই। ■

Example 15: In a ring $(R, +, \bullet)$ prove that $a \bullet 0 = 0$, for all $a \in R$, where 0 is the zero element of R.[1] **(2009.4aiii)**

SOLUTION: আগের অংকটাই। ■

Example 16: Prove that in a ring R we have $a(-b) = (-a)b$ for all $a, b \in R$. **(1999)**

SOLUTION: এই অংকটা ছোটোবেলায় কীভাবে করতে? প্রথমে লিখতে $a(-b) = -(ab)$ আর তারপর লিখতে $(-a)b = -(ab)$. এখানেও ঠিক তাই করব, খালি এই দুটো ধাপকে বিশদ করে লিখব।
$-(ab)$ মানে R-এর সেই element-টা যার সাথে (ab) যোগ করলে 0 হয়। তার মানে $a(-b) = -(ab)$ দেখাতে হলে দেখাতে হবে যে $a(-b) + (ab) = 0$.

> $$\begin{aligned} a(-b) + ab &= a((-b) + b) \quad [\text{by distribution law}] \\ &= a0 \\ &= 0. \end{aligned}$$
>
> So
>
> $$a(-b) = -(ab).$$

এবার একই ভাবে দেখাব $(-a)b = -(ab)$, মানে দেখাব $(-a)b + ab = 0$.

> Similarly,
>
> $$(-a)b + ab = ((-a) + a)b = 0b = 0.$$
>
> So
>
> $$(-a)b = -(ab).$$
>
> Hence
>
> $$a(-b) = (-a)b,$$
>
> as required.

■

Example 17: True or false? Justify. If in a ring R we have $(a+b)^2 = a^2 + 2ab + b^2$ for all a, b then R must be commutative. **(1999,2007)**

SOLUTION:

> The result is true. By property of rings, we have
>
> $$(a+b)^2 = a^2 + ab + ba + b^2.$$

যেহেতু ring-টাকে commutative বলা নেই, তাই ফস্ করে যেন $(a+b)^2 = a^2 + 2ab + b^2$ লিখে বোসো না!

> By the given condition we get
>
> $$a^2 + ab + ba + b^2 = a^2 + 2ab + b^2,$$
>
> or, subtracting $a^2 + ab + b^2$ from both sides,
>
> $$ba = ab.$$

Since this holds for all $a, b \in R$, the ring R must be commutative.

■

Example 18: True or false? Justify. In any ring R

$$(a+b)^2 = a^2 + 2ab + b^2.$$

(1997)
SOLUTION:

The result is false.
By property of a ring,

$$(a+b)^2 = a^2 + b^2 + ab + ba.$$

So the result holds if and only if

$$ab = ba.$$

As a counterexample let R be the ring of all 2×2 real matrices under the usual operations. Take

$$a = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}, b = \begin{bmatrix} 0 & 3 \\ -1 & 2 \end{bmatrix}.$$

Then

$$ab = \begin{bmatrix} -2 & 7 \\ -4 & 17 \end{bmatrix} \neq ba = \begin{bmatrix} 9 & 12 \\ 5 & 6 \end{bmatrix}.$$

■

Example 19: True or false? Justify. In a ring R we have $a^2 - b^2 = (a+b)(a-b)$ for all $a, b \in R$. **(2000)**
SOLUTION: দেখেই মনে হয় যেন উত্তর হবে 'True' কিন্তু একবার ভেবে নেওয়া যাক। স্কুলে যে শিখেছিলাম $(a-b)(a+b) = a^2 - b^2$ তার প্রমাণ ছিল এইরকম--

$$(a-b)(a+b) = a^2 - b^2 + ab - ba = a^2 - b^2.$$

এই যে ab আর ba দিব্যি কেটে গেল, তার কারণ সাধারণ সংখ্যার গুণ হল commutative. কিন্তু এখানে আমরা যেকোনো ring নিয়ে কাজ করছি, ফলে গুণটা commutative নাও হতে পারে।

The result is false.
By property of rings,

$$(a+b)(a-b) = a^2 - b^2 + ab - ba.$$

This equals $a^2 - b^2$ if and only if $ab = ba$.

সুতরাং কোনো non-commutative ring নিলেই counterexample পাওয়া যাবে। আর non-commutative ring-এর সহজ উদাহরণ হল matrix ring.

As a counterexample let R be the ring of all 2×2 real matrices under the usual operations. Take

$$a = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}, b = \begin{bmatrix} 0 & 3 \\ -1 & 2 \end{bmatrix}.$$

Then

$$ab = \begin{bmatrix} -2 & 7 \\ -4 & 17 \end{bmatrix} \neq ba = \begin{bmatrix} 9 & 12 \\ 5 & 6 \end{bmatrix}.$$

কী করে বুঝলাম এই দুটো matrix দিয়েই কাজ হবে? উত্তর হল--মোটামুটি যা খুশি দুটো matrix নিলেই সাধারণতঃ ওরা commute করে না, যদি না matrix দুটো নেহাত সহজ কিছু হয়ে যায়। যদি দুর্ভাগ্যবশতঃ সেরকম কোনো উদাহরণ নিয়ে ফ্যালো, তবে কোনো একটা সংখ্যাকে একটু এদিক ওদিক করে দিলেই হবে। ■

Example 20: R is a ring. $a, b \in R$ and $m, n \in \mathbb{Z}_+$. Show that $(ma)(nb) = (mn)(ab)$. **(2004)**

SOLUTION: প্রথমে বুঝে নিই ঠিক কী দেখাতে বলেছে। R একটা ring আর a, b তার দুটো element. এবার m, n দুটো positive integer নেওয়া হয়েছে, ধর $m = 2$ আর $n = 3$. তাহলে দেখাতে হবে যে $(2a)(3b) = 6(ab)$.
এখানে $2a$ মানে $a + a$ আর $3b$ মানে $b + b + b$. একই ভাবে $6(ab)$ হল ছয়টা ab-র যোগফল। অর্থাৎ দেখাতে হবে যে

$$(a+a)(b+b+b) = ab + ab + ab + ab + ab + ab.$$

ব্র্যাকেট তুলে সরাসরি গুণ করে দিলেই এটা দেখানো যায়। এই কথাটাকেই general m, n দিয়ে লিখব।

$$(ma)(nb) = \underbrace{(a + \cdots + a)}_{m \text{ times}}(nb) = \underbrace{a(nb) + \cdots a(nb)}_{m \text{ times}},$$

by the distribution law.
Similarly,

$$a(nb) = a\underbrace{(b + \cdots + b)}_{n \text{ times}} = \underbrace{ab + \cdots + ab}_{n \text{ times}} = n(ab).$$

So

$$(ma)(nb) = \underbrace{n(ab) + \cdots n(ab)}_{m \text{ times}} = (mn)(ab),$$

as required.

■

Example 21: If $a, b \in R$ and $m, n \in \mathbb{Z}^+$ (set of positive integers), then show that

$$(ma)(nb) = (mn)(ab),$$

where R is a ring.[2] **(2012.3a)**
SOLUTION: আগের অংকটাই। ■

Example 22: In a ring R show that $(a-b)-c = a-(b+c)$ for all $a, b, c \in R$. **(2000,2005,2008)**

SOLUTION: এটাকে একটা "বোকা বোকা" অংক মনে হতে পারে। তোমাকে স্কুলে এই অংকটা দিলে তুমি কী করতে? প্রথমে $(a-b)-c = a-b-c$ লিখতে, কারণ এখানে "ব্র্যাকেটের কোনো দরকার নেই"। তারপর "মাইনাস কমন নিয়ে" লিখতে $a-b-c = a-(b+c)$. এখানে খালি দেখাতে হবে যে ওই "ব্র্যাকেটের কোনো দরকার নেই" আর "মাইনাস কমন নেওয়া" এ দুটো ব্যাপার যে কোনো ring-এর বেলাতেই খাটে। এই প্রসঙ্গে একটা কথা খেয়াল রেখো-- $a-b$ মানে $a+(-b)$.

$$\begin{aligned}(a-b)-c &= (a+(-b))+(-c)\\ &= a+((-b)+(-c)) \quad [\text{ by associativity}]\end{aligned}$$

এবার "মাইনাস কমন নেওয়ার" পালা, মানে দেখাব যে $(-b)+(-c) = -(b+c)$. এর জন্য দেখাব যে $(b+c)+((-b)+(-c)) = 0$ হয়--

Now, using associative law and commutativity of addition

$$(b+c)+((-b)+(-c)) = (b+(-b))+(c+(-c)) = 0+0 = 0.$$

So

$$(-b)+(-c) = -(b+c).$$

সব মিলিয়ে দাঁড়ালো--

So

$$a+((-b)+(-c)) = a+(-(b+c)) = a-(b+c),$$

as required.

■

Exercise 5: একটা অংকে দেখাতে বলেছিল--For all a, b in a ring R, show that $-(a+b) = -a-b$. একজন ছাত্র অংকটা এইভাবে করেছে--

$$-a-b = -1\cdot a+(-1)\cdot b = -1\cdot(a+b) = -(a+b).$$

ও কি ঠিক করেছে? ■

Example 23: True or false? Justify. If x is an idempotent element in a ring R with identity, then $1-x$ is also idempotent. **(2002)**

SOLUTION: এখানে "**idempotent**" বলে একটা শব্দ রয়েছে। একটা ring-এর কোনো element x-কে idempotent বলে যদি $x^2 = x$ হয়, অর্থাৎ element-টা নিজেই নিজের square হয়। Integer-দের ক্ষেত্রে এরকম খালি দুটো সংখ্যা আছে, 1 আর 0. কিন্তু general কোনো ring-এর বেলায় এরকম আরও অনেক idempotent element থাকতে পারে।

> The statement is true.
>
> Given: $x^2 = x$.
>
> $$\begin{aligned} (1-x)^2 &= 1^2 + x^2 - 1x - x1 \\ &= 1 + x^2 - x - x \\ &= 1 + x - x - x \quad [\because x^2 = x] \\ &= 1 - x, \end{aligned}$$
>
> as required.

■

Example 24: Let $(R, +, \bullet)$ be a ring and let $x \in R$. If there exists a unique $a \in R$ such that $xa = x$, then prove that $ax = x$.[2] **(2009.4aii)**

SOLUTION: এই রকম অংকে, যেখানে কোনো কিছুকে unique বলা থাকে, সেখানে একটা কায়দা খুব কাজে লাগে। আমাদের দেখাতে হবে $ax = x$, মানে $ax - x = 0$. আমরা করব কি, এই $ax - x$-টাকে a-র সঙ্গে যোগ করে $b = a + ax - x$ বানাব। যেহেতু $ax - x = 0$ হওয়ার কথা তাই এটা আসলে a-ই। কিন্তু সেটা আমরা এখনই ধরে নিতে পারছি না। আমরা দেখাব যে, এই জিনিসটাও a-র শর্তটা পালন করে, মানে $xb = x$ হয়। ব্যস্, অমনি a-র uniqueness থেকে বলা যাবে যে $a = b$. তা থেকেই প্রমাণ হয়ে যাবে $ax - x = 0$.

> Consider $b = a + ax - x \in R$.
>
> Then $xb = x$.
>
> ⟦ <u>Because:</u>
>
> $$\begin{aligned} xb &= x(a + ax - x) \\ &= xa + xax - x^2 \\ &= x + x^2 - x^2 \quad [\because xa = x] \\ &= x. \end{aligned}$$
>
> ⟧
>
> Hence, by uniqueness, $a = b$, ie, $a = a + ax - x$,
>
> or $ax - x = 0$ or $ax = a$, as required.

■

নীচের অংকটাও একইরকম।

Exercise 6: In a ring R there is a unique element e such that $\forall x \in R \quad xe = x$. Show that e must be the unity in R. ■

Exercise 7: একজন ছাত্র উপরের অংকটা করার জন্য Example 24 ব্যবহার করেছে এই ভাবে--

> বলা আছে যে $xe = x$ আর e হল unique. সুতরাং Example 24 থেকে পাই $ex = x$. সুতরাং $\forall x \in R \quad xe = ex = x$ হচ্ছে, এবং তার মানেই তো e হচ্ছে R-এর unity!

এই যুক্তিটা ভুল। কেন? ■

DAY 10
Ring (part 4)

10.1 একটু কম সহজ কিছু অংক

গতকালের অংকগুলোতে যা দেখাতে বলেছিল সেগুলো দেখেই বোঝা যাচ্ছিল কী করে দেখাতে হবে, খালি definition-গুলো মাথায় রেখে লিখে যাওয়ার অপেক্ষা। এবারের অংকগুলো তার চেয়ে একটু বেশী কঠিন। কোন পথে এগোতে হবে সেটা আগে ভালো করে ভেবে নেওয়া দরকার।

Example 25: True or false: If in a ring R, $a^2 = a$ for all $a \in R$ then $2a = 0$. **(1998,2005,2007,2010)**

SOLUTION:

> The result is true.

অবশ্যই এটা আমরা প্রথমেই কোনো আশ্চর্য উপায়ে বুঝে ফেলিনি। আগে আমরা বেশ কয়েকবার খাবি খেয়ে নীচের ধাপগুলো কষে দেখেছি, তারপর অংকটা মিলে যাবার পরে উপরের লাইনটা লিখেছি।
শুরুতে খালি জানতাম যে, R-এর সব element-ই তার নিজের square-এর সমান। দেখতে হবে $a \in R$ হলেই $2a = 0$ হবে কিনা।

> Take any $a \in R$. Then
>
> $$\begin{aligned} 2a &= a + a \\ &= (a+a)^2 \quad \left[\text{by the given condition}\right] \\ &= a^2 + a^2 + aa + aa \\ &= a + a + a + a \quad \left[\text{by the given condition}\right] \\ &= 4a. \end{aligned}$$
>
> Subtracting $2a$ from both sides,
>
> $$2a = 0,$$

as required.

কী করে বুঝলাম যে ঠিক এই ধাপগুলোই করতে হবে? এর উত্তর হচ্ছে-- এদিক ওদিক খানিকক্ষণ ঢুঁ মেরে! বলা ছিল যে, সবাই নিজের square-এর সমান। হাতের কাছে $2a$ রয়েছে, তাই ওটাকেই square করে পেলাম $2a = 4a^2$. এবার a^2-টা দেখে মনে হল ওটাকে তো a হিসেবে লেখা যায়, তাতেই দেখি অংকটা হয়ে গেল। এবার খালি $2a$-কে square করলে কেন $4a^2$ হয় সেটাকে বিশদ করে লিখেছি, কারণ হাজার হোক এখানে তো আর আমরা সাধারণ সংখ্যা নিয়ে কাজ করছি না, এখানেও যে 2-এর square করলে 4-ই হয় সেটা একটু বুঝিয়ে দেওয়াই ভালো। ■

Example 26: Let R be a ring. Then prove that if $\forall a \in R$ we have $a^2 = a$ then R is a commutative ring. **(1997)**

SOLUTION:

Given: $\forall a \in R \ a^2 = a$.

To Show:

$\forall x, y \in R \quad xy = yx$.

$\forall x, y$

Take any $x, y \in R$.

Then

$$(x+y)^2 = x^2 + y^2 + xy + yx.$$

এইখানে সাবধান, ফস্ করে $(x+y)^2 = x^2 + y^2 + 2xy$ লিখে বোসো না যেন, কারণ আমাদের R-টা যে commutative হবে সেটা তো এখনও দেখানো শেষ হয় নি। তাই $xy + yx$ যে $2xy$-এর সমান হবে, এখনই সেটা ধরে নিতে পারি না!

or, since $\forall a \in R \quad a^2 = a$,

$$x + y = x + y + xy + yx.$$

Subtracting $x + y$ from both sides,

$$0 = xy + yx,$$

or

$$xy = -yx$$

এখন বলা আছে যে, সবাই নিজের square-এর সমান। তাই আমরা দুই দিককে square করে দিলেই বাঁদিকে xy-ই থাকবে। আর ডানদিকে লক্ষ করো যে, $-yx$-এর square আসলে yx-এর square (যেমন -2 আর 2 দুজনেরই square হল 4)। সুতরাং ডানদিকে তাহলে পাব yx. ব্যস্, তাহলেই হয়ে যাবে--

Squaring both sides, $(xy)^2 = (-yx)^2$.

Now by the given condition, $(xy)^2 = xy$.

Also $(-yx)^2 = (yx)^2 = yx$.

So we have $xy = yx$, as required.

■

Example 27: If in a ring $(B, +, \cdot)$, $a^2 = a$ for all $a \in B$, show that $2a = a + a = 0$ for all a, where B is a commutative ring. Show that in a commutative ring R, $2a = 0$ for all $a \in R$ need not hold.[3] **(2010.4aii)**

SOLUTION: প্রথম অংশ তো আগেই করেছি Example 25-এ। এবার দ্বিতীয় অংশ--

> Second part: Counterexample: The ring $(\mathbb{Z}, +, \cdot)$ is commutative. But taking $a = 1$, we see $2 \times 1 = 2 \neq 0$.

■

Example 28: Define the characteristic of a ring. If in a ring R with more than one element $a^2 = a$ for all $a \in R$, then show that the characteristic of R is 2. Is this ring commutative? Justify. **(2003)**

SOLUTION:

> DEFINITION: **Characteristic of a ring**
>
> The characteristic of a ring is defined as the smallest positive integer n such that
>
> $$\forall a \in R \quad \underbrace{a + \cdots + a}_{n \text{ times}} = 0.$$
>
> If no such positive integer exists, then the characteristic is defined to be 0.
>
> For example, $\mathbb{Z}_3$ has characteristic 3 and $\mathbb{Z}$ has characteristic 0.

এবার দ্বিতীয় অংশ--

> Since R has more than one element, so it contains a nonzero element. Hence its characteristic cannot be 1.

কারণ একমাত্র একা ring-এরই characteristic হয় 1, সেটা হল trivial ring, মানে যার মধ্যে 0 ছাড়া আর কিচ্ছু element নেই।

> So to prove that R has characteristic 2, it is enough to show that $\forall a \in R$ $2a = 0$.

ঠিক এইটাই আমাদের প্রমাণ করতে বলা হয়েছিল Example 25-এ। সুতরাং এবার ওই অংকের সমাধানটা জুড়ে দিলেই চলবে। ■

Example 29: If in a ring $(R, +, \bullet)$ $a^2 = a$ for all $a \in R$ then show that the ring has characteristic 2. Further show that $(a+b)^2 = a^2 + b^2$ for all $a, b \in R$.[2+3] **(2007)**

SOLUTION: প্রথম অংশটার সমাধান তো আগের অংকেই করলাম। এবার দ্বিতীয় অংশটা করি--

> Second part: Since every element of R equals its own square,
>
> $$(a+b)^2 = a+b = a^2+b^2,$$
>
> as required.

■

Example 30: Let $(R, +, \bullet)$ be a ring with unity such that $(xy)^2 = x^2y^2$ for all $x, y \in R$. Prove that R is a commutative ring.[5] **(2009.4b)**

SOLUTION: দেওয়া আছে $(xy)^2 = x^2y^2$, মানে $xyxy = xxyy$. তাই ফস্ করে মনে হতে পারে যে, বাঁদিক থেকে x আর ডানদিক থেকে y কেটে নিলেই তো বেশ $yx = xy$ হয়ে যায়। কিন্তু সাবধান, এটা একটা ring, এখানে ওই "কেটে নেওয়া"-টা নাও চলতে পারে।

অংকটা সামান্য ঘুরপথে করব। প্রথমেই commutative না দেখিয়ে একটা অন্য জিনিস দেখাব। ঘুরপথটা কয়েকবার এদিক ওদিক ঢুঁ মেরে বার করতে হয়েছে।

> Step 1: Shall show
>
> ◎ $\forall a, b \in R \quad aba = a^2b.$
>
> $\forall a, b$ Take any $a, b \in R$.
>
> Putting $x = a$ and $y = 1 + b$ in the given condition,
>
> $$(a(1+b))^2 = a^2(1+b)^2,$$
>
> or
>
> $$(a+ab)^2 = a^2(1+2b+b^2),$$
>
> or
>
> $$a^2 + (ab)^2 + a^2b + aba = a^2 + 2a^2b + a^2b^2.$$
>
> Now we have $(ab)^2 = a^2b^2$. So
>
> $$aba = a^2b,$$
>
> as required. Thus
>
> $$\forall a, b \in R \quad aba = a^2b. \qquad (*)$$

এটাকে একটা লেবেল দিয়ে রাখলাম, কারণ পরে কাজে লাগবে। এইবার আমরা commutative দেখাব--

Step 2: Shall show

$\forall p, q \in R \quad pq = qp.$

$\forall p, q$ Take any $p, q \in R$.

Then putting $a = 1 + p$ and $b = q$ in (*),

$$(1+p)q(1+p) = (1+p)^2 q,$$

or

$$q + pq + qp + pqp = q + 2pq + p^2 q,$$

or

$$qp + pqp = pq + p^2 q.$$

Now by (*) we know that $pqp = p^2 q$. So we have

$$qp = pq,$$

as required.

■

Example 31: If R is a ring and $e \in R$ such that $e^2 = e$ then show that

$$(xe - exe)^2 = (ex - exe)^2$$

for every $x \in R$. **(1999)**

SOLUTION:

$$\begin{aligned} LHS &= (xe - exe)^2 \\ &= (xe)^2 + (exe)^2 - xeexe - exexe \\ &= xexe + exe^2xe - xe^2xe - exexe \\ &= xexe + exexe - xexe - exexe \quad [\because e^2 = e] \\ &= 0. \end{aligned}$$

Similarly,

$$\begin{aligned} RHS &= (ex - exe)^2 \\ &= (ex)^2 + (exe)^2 - exexe - exeex \\ &= exex + exe^2xe - exexe - exe^2x \\ &= exex + exexe - exexe - exex \quad [\because e^2 = e] \\ &= 0. \end{aligned}$$

Thus, $LHS = RHS$, as required.

■

এবার একটা অংক করব যেটা নিছক কিছু কসরৎ মাত্র। Ring শেখার জন্য এর গুরুত্ব সামান্যই।

Example 32: True or false? Justify. If in a ring R we have two elements a, b such that $ab + ba = 1$ and $a^3 = a$ then $a^2 = 1$. **(1998,2007)**

SOLUTION: আচ্ছা, $a^3 = a$-র দুদিক থেকে একটা a কেটে নিলেই তো দিব্যি $a^2 = 1$ হয়ে যায়। তবে আবার কষ্ট করে $ab + ba = 1$ কেন দিয়েছে? কারণ, এটা একটা ring-এর অংক, অতএব ইচ্ছে করলেই দুদিক থেকে a কেটে নেওয়া নাও যেতে পারে। এখানে যে কাটা যাবে সেটা দেখানোর জন্যই ওই $ab + ba = 1$-টা দরকার।

The result is true. Given,

$$ab + ba = 1. \quad (\mathbf{1})$$

Multiplying both sides by a^2 from the left,

$$a^3b + a^2ba = a^2,$$

or, since $a^3 = a$,

$$ab + a^2ba = a^2,$$

or

$$a^2 = ab + a(ab)a = ab + a(1 - ba)a = ab + a^2 - aba^2,$$

or

$$ab - aba^2 = 0,$$

or

$$ab(1 - a^2) = 0. \quad (\mathbf{2})$$

Now, multiplying both sides of $(\mathbf{1})$ with $(1 - a^2)$ from the right,

$$ab(1 - a^2) + ba(1 - a^2) = 1 - a^2.$$

By $(\mathbf{2})$, $ab(1 - a^2) = 0$. Also

$$ba(1 - a^2) = ba - ba^3 = ba - ba = 0,$$

since $a^3 = a$.

So $1 - a^2 = 0$, or $a^2 = 1$, as required.

■

Exercise 8: Let x be a nonzero element of a ring R with unity 1. If there exists a unique $y \in R$ such that $xyx = x$ then prove that $xy = 1 = yx$.[3] **(2010.4bii)**

HINT:

কোনো কিছুকে unique বলে দেওয়া থাকলে সেটাকে ব্যবহার করে কোনো দুটো জিনিসকে সমান দেখানোর একটা কায়দা আছে, যেটা আমরা আগেও একবার ব্যবহার করেছি। আরেকবার মনে করিয়ে দিই। ধরো প্রথমে $xy = 1$ দেখাব, মানে $xy - 1 = 0$ দেখাব। আমরা এই $xy - 1$-টাকে y-এর সঙ্গে যোগ করে পাব--

> Let $z = y + xy - 1$.

এবার দেখাব যে, এই z-টাও y-এর শর্তটা পালন করে, মানে $xzx = x$ হয়। তাহলেই uniqueness থেকে পেয়ে যাব $z = y$, মানে $xy - 1 = 0$.

> Then
>
> $$\begin{aligned} xzx &= x(y + xy - 1)x \\ &= xyx + x^2yx - x^2 \\ &= x + x(xyx) - x^2 \quad [\because xyx = x] \\ &= x + x^2 - x^2 \quad [\because xyx = x] \\ &= x. \end{aligned}$$
>
> So by the uniqueness condition, we must have $y = z$, ie $y = y + xy - 1$, ie, $xy = 1$, as required.

এবার একইভাবে $yx = 1$ দেখাও দেখি। ■

10.2 আরও কঠিন কিছু অংক

এবার কিছু কঠিন অংক দিই মগজ খাটাবার জন্য। কিন্তু গোড়াতেই সাবধান। এই অংকগুলো খালি মগজের কসরৎ ছাড়া আর কিছুই নয়। এগুলোর কোনো গুরুত্বপূর্ণ প্রয়োগ নেই। এবং খানিকটা আন্দাজে হাতড়ানোরও প্রয়োজন হতে পারে। যদি নিছক ধাঁধা হিসেবে করতে ভালো লাগে, তবেই করো, নইলে বাদ দিয়ে দাও।

Exercise 9: Let $(R, +, \bullet)$ satisfy all conditions of a ring with unity except possibly commutativity of addition. Prove that $(R, +, \bullet)$ must be a ring.
HINT:
চট্ করে বুঝে নিই কী করতে বলছে। $(R, +, \bullet)$-র উপর ring-এর সংজ্ঞার সব শর্তই দেওয়া আছে, খালি addition-এর commutativity ছাড়া। মানে এটা বলা নেই যে $a, b \in R$ হলেই $a + b = b + a$ হবে। কিন্তু তার বদলে দেওয়া আছে যে R-এর মধ্যে unity আছে, অর্থাৎ এমন একটা $1 \in R$ আছে, যাতে

$$\forall a \in R \quad 1 \bullet a = a \bullet 1 = a$$

হয়। এ থেকে তোমাকে দেখাতে হবে যে addition-টা আসলে commutative হতে বাধ্য, মানে

$$\forall a, b \in R \quad a + b = b + a.$$

এর জন্য $(a + b) \bullet (1 + 1)$-কে দুভাবে বার কর। একবার $(a + b) \bullet (1 + 1) = (a + b) \bullet 1 + (a + b) \bullet 1$ করে, অন্যবার $(a + b) \bullet (1 + 1) = a \bullet (1 + 1) + b \bullet (1 + 1)$ করে। যে দুটো জিনিস পাবে এরা দুজনে দেখতে আলাদা হলেও আসলে সমান। দ্যাখো কিছু কাটাকাটি হয় কিনা। ■

Exercise 10: Let R be a ring with unity. Let $a, b \in R$ be such that $1 - ab$ is a unit. Show that $1 - ba$ must also be a unit.

HINT:
এখানে খানিকটা হাতড়াতে হবে। ধরো x হল $(1+ab)$-এর multiplicative inverse. তাহলে তোমার হাতে এখন চারটে element আছে--$1, a, b$, আর x. এদেরকে মিলিয়ে-জুলিয়ে $1-ba$-এর একটা multiplicative inverse খাড়া করতে হবে। ■

DAY 11
Ring (part 5)

11.1 Zero divisor

আমরা স্কুলে থাকতে এরকম অংক আকছার করেছি--

$x^2-5x+6=0$ হলে $x=?$

এর জন্য প্রথমে factorise করে নিতে হত--

$$(x-3)(x-2)=0.$$

তার পর আমরা বলতাম যে $(x-3)$ আর $(x-2)$-র গুণফল যখন 0, তার মানে ওদের মধ্যে অন্ততঃ একজন 0 না হয়ে যায় না। তাই $x=2$ বা 3. এইখানে আমরা একটা তথ্য ব্যবহার করলাম যে, দুটো real number-এর গুণফল শূন্য হলে ওদের মধ্যে অন্ততঃ একজন শূন্য হবেই। ঘুরিয়ে বললে বলা যায় যে, যদি $x, y \in \mathbb{R}$ হয় তবে $x \neq 0, y \neq 0$ হলে অবশ্যই $xy \neq 0$ হবে। দুঃখের কথা, এই চমৎকার জিনিসটা অনেক ring-এর বেলাতেই খাটে না। এমন বিচ্ছিরি ring সম্ভব যেখানে দুটো nonzero element-এর গুণফল zero হয়! (এখানে zero বলতে ring-টার additive identity বোঝানো হচ্ছে)। এরকম nonzero element-দের বলে **zero divisor**
একটা উদাহরণ এইরকম--

$$\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \times \begin{bmatrix} 0 & 2 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

বাঁদিকে দুটো matrix-ই nonzero, অথচ ওদের গুণ করে পাচ্ছি zero matrix. তাই বাঁদিকের দুটো matrix-কে বলব একেকটা zero divisor. আরও খুঁটিয়ে বললে প্রথম matrix-টাকে বলব একটা left zero divisor, কারণ ওটা গুণ চিহ্নটার বাঁদিকে রয়েছে, আর অন্যটাকে বলব একটা right zero divisor. অংকের ভাষায় সংজ্ঞাটা এইরকম--

> DEFINITION: **Left and right zero divisor**
>
> Let $(R, +, \bullet)$ be a ring. Then $a, b \in R$ be such that $a, b \neq 0$, but $a \bullet b = 0$. Then a is called a **left zero divisor** and b is called a **right zero divisor** in R.

নীচের অংকে zero divisor-ওয়ালা ring-এর একটা উদাহরণ রয়েছে।

Example 33: Is the ring $(\mathbb{Z} \times \mathbb{Z}, +, \bullet)$ commutative? Does it contain divisors of zero? Justify your answer. [The addition and multiplication operations are defined as $(a,b)+(c,d)=(a+c,b+d)$ and $(a,b) \bullet (c,d) = (ac, bd)$ for $(a,b),(c,d) \in \mathbb{Z} \times \mathbb{Z}$.][3] **(2008)**
SOLUTION:

> Yes, the ring is commutative, since $\forall (a,b),(c,d) \in \mathbb{Z}\times\mathbb{Z}$ we have
> $$(a,b)\bullet(c,d) = (ac,bd) = (ca,db) = (c,d)\bullet(a,b),$$
> because multplication in $\mathbb{R}$ is commutative.

মনে রেখো, একটা ring-কে commutative দেখানোর মানে তার গুণটাকে commutative দেখানো। যোগটা তো এমনিতেই commutative.

> Yes, it contains divisors of zero.
> For example, $(1,0),(0,1) \in R$ are both nonzero, but
> $$(1,0)\bullet(0,1) = (1\times 0, 0\times 1) = (0,0).$$

■

Example 34: True or false? Justify. A ring has always a divisor of zero.[2] **(2007)**

SOLUTION:

> The statement is false.
> For example, $(\mathbb{Z},+,\cdot)$ is a ring without any zero divisor, because if $\forall m,n\in\mathbb{Z}$ $m,n\neq 0 \implies m\cdot n\neq 0$.

■

নীচের অংকটা ring-এর গুণ করার cancellation law নিয়ে, মানে $ab = ac$ দেওয়া থাকলে বাঁদিক থেকে a-কে "কেটে নিয়ে" $b = c$ লেখা যায় কিনা। যদি যায় তবে বলব যে, সেই ring-এর গুণের বেলায় left cancellation law খাটে। একইভাবে $ba = ca$ থেকে $b = c$ বলা গেলে বলব right cancellation law খাটে। অবশ্য সব ring-এর বেলায় সেটা খাটে না। যেমন ধরো matrix-দের বেলায়--

$$\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \times \begin{bmatrix} 0 & 2 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \times \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

হয় বটে, কিন্তু তা বলে তুমি $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$-টাকে কেটে নিয়ে বলতে পারো না যে $\begin{bmatrix} 0 & 2 \\ 0 & 0 \end{bmatrix}$ আর $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ হল সমান! এই উদাহরণটা থেকেই আন্দাজ করতে পারছ হয়তো যে, cancellation law আর zero divisor-এর অস্তিত্বের মধ্যে একটা সম্পর্ক আছে। সেটা নিয়েই এবারের অংকটা।

Example 35: Prove that a ring R has no zero divisors if and only if the cancellation laws for multiplication hold in R. **(2000)**

SOLUTION:

The cancellation laws are:

$$\forall a, b, c \in R(ab = ac \quad \& \quad a \neq 0) \implies b = c,$$

and

$$\forall a, b, c \in R(ba = ca \quad \& \quad a \neq 0) \implies b = c.$$

To show:

No zero divisor $\iff$ cancellation laws hold.

`` $\implies$ " part:

Let R have no zero divisor.

এবার দেখাব যে cancellation law দুটো খাটতে বাধ্য।

Take any $a, b, c \in R$ such that $ab = ac$ and $a \neq 0$. Then $ab - ac = 0$, or $a(b - c) = 0$.

Since there is no zero divisor and $a \neq 0$, so $b - c = 0$, or $b = c$.

So left cancellation law holds.

Similarly, if $a, b, c \in R$ are such that $ba = ca$ and $a \neq 0$, then

$$(b - c)a = 0 \implies b - c = 0,$$

since there is no zero divisor and $a \neq 0$.

So $b = c$.

Thus, right cancellation law holds.

` $\impliedby$ ' part:

Let $a \neq 0$ and $ab = 0$ Then shall show that $b = 0$.

This is because

$$ab = 0 \implies ab = a0,$$

and hence, cancelling a from left, $b = 0$, as required.

Similarly, if $a \neq 0$ and $ba = 0$, then

$$ba = 0 \implies ba = 0a,$$

and so, cancelling a from right, $b = 0$, as required.

■

Example 36: Let $M_2(\mathbb{R})$ denote the ring of all 2×2 matrices over the field of real numbers under usual matrix addition and matrix multiplication. Show that this is a non-commutative ring with identity and with zero divisors. **(1999)**

SOLUTION: Ring তো দিয়েই দিয়েছে, খালি দেখাতে হবে non-commutative, identity আর zero divisor.

> Non-commutative:
> $$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} = \begin{bmatrix} 3 & 4 \\ 1 & 2 \end{bmatrix},$$
> but
> $$\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 4 & 3 \end{bmatrix} \neq \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}.$$
> Identity:
> The matrix
> $$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$
> is the identity element of $M_2(\mathbb{R})$, because
> $$\forall A \in M_2(\mathbb{R}) IA = AI = A.$$
> Zero divisors:
> The matrix $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$ is nonzero, but
> $$\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 0 & 2 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$
> Thus $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$ is a left zero divisor, and $\begin{bmatrix} 0 & 2 \\ 0 & 0 \end{bmatrix}$ is a right zero divisor.

■

Example 37: True or false? Justify. The matrix ring $M_2(\mathbb{R})$ has zero divisors. $M_2(\mathbb{R})$ denotes the set of all 2×2 matrices over $\mathbb{R}$.[2] **(2001)**

SOLUTION:

> The statement is true.

একটা উদাহরণ আমরা এক্ষুণি দিলাম আগের অংকটায়। ■

Example 38: Show that the matrix ring $M_2(\mathbb{R})$ has zero divisors.[2] **(2009.4cii)**

SOLUTION: আগের অংকেই করা হয়েছে। ■

Example 39: R is a (commutative) ring with unity 1, having no zero divisors and if for $a, b \in R$ $ab = 1$ then show that $ba = 1$. **(2003,2008,2006)**

SOLUTION:

> We first assume $0 \neq 1$.

এইটা দেখে থতমত খেয়ে যাওয়া অদ্ভুত নয়। 0 যে 1 নয়, এতে আবার "assume" করার কী আছে, বাপু? আসলে বিশ্বে এমন একটা (এবং একটাই) ring আছে যেখানে $0 = 1$. তাকে বলে **trivial ring.** সেই প্রসঙ্গে এক্ষুণি আসছি, আগে $0 \neq 1$ হলে কী করে এগোব সেটা বলি--

> Given
> $$ab = 1.$$
> Multiplying by a from the right,
> $$aba = a,$$
> or
> $$aba - a = 0,$$
> or
> $$a(ba - 1) = 0.$$

এবার যদি কোনোমতে দেখাতে পারি যে $a \neq 0$ তবেই কেল্লা ফতে, কারণ তাহলে $ba - 1 = 0$ হতে বাধ্য, যেহেতু ring-টায় কোনো zero divisor নেই।

> Now, since $ab = 1$ we must have $a \neq 0$ $(\because 1 \neq 0)$.
> Since the ring has no zero divisor, we must have $ba - 1 = 0$, or $ba = 1$, as required.

সবশেষে trivial ring-এর কেসটা বলি। এরকম ring-এ খালি একটাই element সেটাই একাধারে 0 এবং 1. সুতরাং--

> If the ring is trivial, then $a = b = 0 = 1$, and so the result is obvious.

■

Example 40: Give an example (with justification) of a commutative ring without identity element and without zero divisor.[2] **(2009.4ai)**

SOLUTION:

> $(2\mathbb{Z}, +, \cdot)$ is a commutative ring without identity element and without zero divisors.
> We know that $(\mathbb{Z}, +, \cdot)$ is a ring. Now $2\mathbb{Z}$ is its subring.
>
> ⟦ Because:
>
> 1) $\because 0 \in 2\mathbb{Z}$ $\therefore 2\mathbb{Z} \neq \phi$.
> 2) If $a, b \in 2\mathbb{Z}$ then $a - b$ is again an even number, $\therefore a - b \in 2\mathbb{Z}$.
> 3) If $a, b \in 2\mathbb{Z}$, then ab is also an even number, $\therefore ab \in 2\mathbb{Z}$.

]]

$\mathbb{Z}$ has no zero divisor, so $2\mathbb{Z}$ also does not have any zero divisor.

Also, $2\mathbb{Z}$ does not have any identity.

[[Because:

Let, if possible, $n \in 2\mathbb{Z}$ be identity. Then
$\forall k \in 2\mathbb{Z} \quad kn = k$.
In particular, for $k = 2,\ 2n = 2$. So $n = 1 (\Rightarrow\Leftarrow \because 1 \notin 2\mathbb{Z})$.

]]

■

Example 41: True or false? Justify. If a ring contains a left zero divisor then it contains a both-sided zero divisor. **(2006)**

SOLUTION: Both-sided zero divisor মানে এমন একটা element যেটা একাই সঙ্গে left এবং right zero divisor.

The result is true. Let $a \in R$ be a left zero divisor, ie, $a \neq 0$ and $\exists b \in R$, $b \neq 0$, such that $ab = 0$. Consider ba.

If $ba = 0$, then a is also a right zero divisor, and hence a both sided zero divisor. If $ba \neq 0$ then it is a both sided zero divisor, because

$$a(ba) = (ab)a = 0a = 0$$

and

$$(ba)b = b(ab) = b0 = 0.$$

■

11.2 Unit

Unit কাকে বলে সেটা তো আগেই বলেছি--একটা ring-এর মধ্যে যদি multiplicative identity থাকে তবে যে সব element-এর multiplicative inverse আছে তাদের বলে **unit.**

Example 42: In the ring $(\mathbb{Z}_n, +, \bullet)$ if an element $\bar{m}$ is unit then show that $gcd(m, n) = 1$.[2] **(2007)**

SOLUTION:

Let $\bar{m}$ be a unit in $\mathbb{Z}_n$.

Then $\exists \bar{k} \in \mathbb{Z}_n$ such that $\bar{m} \bullet \bar{k} = \bar{1}$,

ie,

$$mk \equiv 1 \pmod{n},$$

ie,

$$mk = 1 + ln \text{ for some } l \in \mathbb{Z}.$$

So

$$mk - ln = 1.$$

Let $d = gcd(m, n)(> 0)$ then $d|m, n$ and so

$$d|mk - ln = 1.$$

So $d = 1$, as required.

■

এই অংকটার converse-টাও কিন্তু ঠিক। সেটা দেখাতে বলেছে নীচের অংকটায়।

Exercise 11: Let $\bar{m} \in \mathbb{Z}_n$ be such that $gcd(m, n) = 1$. Then show that $\bar{m}$ must be a unit in the ring $\mathbb{Z}_n$. ■

এই অংকটারই একটা প্রয়োগ দিয়েছে এবার।

Exercise 12: Find the elements of the ring $(\mathbb{Z}_{12}, +_{12}, \bullet_{12})$ which are zero divisors.[2] **(2010.4bi)**
HINT: এখানে $+_{12}$ মানে হল modulo 12 যোগ, আর $\bullet_{12}$ মানে modulo 12 গুণ। তোমাকে দেখতে হবে $0, 1, 2, ..., 11$-র মধ্যে কারা কারা 12-র সঙ্গে **relatively prime**, মানে এরকম কী কী $x \in \{0, 1, ..., 11\}$ আছে যাতে $gcd(x, 12) = 1$ হয়। ■

Example 43: In a ring with unity if a and b are units, prove that ab is also a unit.[3] **(2012.3b)**

SOLUTION:

Given $a, b \in R$ are units, where R is a ring with unity.

To show

◎ $\exists c \in R \quad (ab)c = 1$ and $c(ab) = 1$.

Since a, b are units in R,

so $\exists a^{-1}, b^{-1} \in R \; aa^{-1} = a^{-1}a = 1$ and $bb^{-1} = b^{-1}b = 1$.

$\because R$ is closed under multiplication,

$\therefore b^{-1}a^{-1} \in R$.

$\forall c$ Choose $c = b^{-1}a^{-1} \in R$.

Then

$$\begin{aligned}(ab)c &= (ab)(b^{-1}a^{-1})\\ &= a(bb^{-1})a^{-1}\\ &= a1a^{-1}\\ &= aa^{-1}\\ &= 1,\end{aligned}$$

as required.

Similarly,

$$\begin{aligned}c(ab) &= (b^{-1}a^{-1})(ab)\\ &= b^{-1}(a^{-1}a)b\\ &= b^{-1}1b\\ &= b^{-1}b\\ &= 1,\end{aligned}$$

as required.

■

Example 44: R is a ring with unity. If $a \in R$ is a unit, then show that a is not a zero divisor.[3] **(2004,2007)**

SOLUTION:

Let $a \in R$ be a unit. Let, if possible, a be a zero divisor. Then

$$\exists b \in R \quad b \neq 0 \text{ and } \big(ab = 0 \text{ or } ba = 0\big).$$

এখানে আমরা $ab = 0$ আর $ba = 0$ দুটো সম্ভাবনাই রেখেছি, কারণ a-টা left zero divisor হবে নাকি right zero divisor হবে সেটা বুঝতে পারছি না।

Since a is a unit, $\exists a^{-1} \in R$ such that $aa^{-1} = a^{-1}a = 1$. If $ab = 0$ then multiplying from the left with a^{-1} we have

$$a^{-1}ab = a^{-1}0,$$

or

$$b = 0(\Rightarrow\Leftarrow \because b \neq 0).$$

Similarly if $ba = 0$ then

$$b = baa^{-1} = 0a^{-1} = 0(\Rightarrow\Leftarrow).$$

■

Example 45: True or false? Justify. If u has an inverse in a ring R with unity, then $-u$ has an inverse too. **(2006)**

SOLUTION: এখানে কী হচ্ছে বোঝার জন্য একটা উদাহরণ নিলে সুবিধা হবে। ধরো R হল আমাদের অতি পরিচিত $\mathbb{R}$, মানে real number-দের ring, আর $u = 2$. তাহলে $u^{-1} = \frac{1}{2}$. অমনি আমরা জানি যে, $-u = -2$-এর inverse হবে $-\frac{1}{2}$. সুতরাং u-এর inverse থাকলেই $-u$-এরও inverse থাকতে বাধ্য।

> The result is true. We know that $\forall a, b \in R$
>
> $$a(-b) = (-a)b = -ab$$
>
> and
>
> $$-(-a) = a.$$
>
> Let v be an inverse of u. Thus
>
> $$uv = vu = 1.$$
>
> So $(-v)(-u) = -(v(-u)) = vu = 1$. Similarly $(-u)(-v) = -(u(-v)) = uv = 1$.

■

DAY 12
Integral domain

আমরা দেখেছি যে $(\mathbb{Z}, +, \bullet)$ হল একটা ring. কিন্তু $\mathbb{Z}$ নিয়ে অংক করা যত সহজ, যেকোনো ring নিয়ে অংক করা তত সহজ নয়। কারণ $\mathbb{Z}$-এর কিছু বাড়তি সুবিধা আছে--

- $\mathbb{Z}$-এর গুণটা commutative,
- $\mathbb{Z}$-এর মধ্যে unity আছে,
- $\mathbb{Z}$-এ কোনো zero divisor নেই।

যদি কোনো ring-এর এইসব গুণ থাকে, তবে তাকে নিয়ে কাজ করা সুবিধা। কারণ স্কুল থেকেই $\mathbb{Z}$-এর যে সব বৈশিষ্ট্য শিখেছি সেগুলো নিশ্চিন্তে লাগিয়ে দেওয়া যায়। তবে একটা ring আছে, যেটা এই তিনটে গুণ থাকা সত্ত্বেও হাস্যকর রকমের মামূলী। সেটা হল $(\{0\}, +, \bullet)$. একে বলে **trivial ring** এর মধ্যে খালি একটাই element আছে, সেটা হল 0. সুতরাং $0 + 0 = 0$ এবং $0 \bullet 0 = 0$. বলাই বাহুল্য যে এটা commutative. এখানে 0 নিজেই unity-র ভূমিকা পালন করছে। আর zero divisor নেই, কারণ কোনো nonzero element-ই তো নেই! সুতরাং আপাতঃদৃষ্টিতে $\mathbb{Z}$-এর ভালো ভালো গুণগুলো সত্ত্বেও এই ring-টা $\mathbb{Z}$-এর থেকে সম্পূর্ণ আলাদা।
এই তুচ্ছ কেসটা বাদ দিলে যে ring-গুলো পড়ে থাকে তাদের নিয়ে কাজ করার সুবিধা বেশী। এদেরকে আমরা বলি **integral domain**

Example 46: Define integral domain. **(1998,2000,2002,2004,2005,2007)**

SOLUTION:

DEFINITION: Integral domain

A ring R is called an integral domain if all the following conditions are satisfied:

- it is commutative,
- it has unity,
- it has no zero divisor,
- it is nontrivial.

■

Integral domain-এর সবচেয়ে সহজ কয়েকটা উদাহরণ হল $(\mathbb{Z}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$ এবং $(\mathbb{C}, +, \cdot)$. আরেক ধরণের গুরুত্বপূর্ণ উদাহরণের হদিশ আছে নীচের অংকটায়।

Example 47: Prove that the ring $(\mathbb{Z}_n, +, \cdot)$ is an integral domain if and only if n is a prime.[4]

(2010.5bii)

SOLUTION: আমরা $\mathbb{Z}_n$ নিয়ে আগেও কাজ করেছি। তখন আমরা লিখেছিলাম $\mathbb{Z}_n = \{0, ..., n-1\}$ আর binary operation দুটো নিয়েছিলাম $\oplus$ (মানে modulo n যোগ) এবং $\odot$ (মানে modulo n গুণ)। এখানে এই দুটো operation-কেই '$+$' আর '$\cdot$' দিয়ে বুঝিয়েছে। পাছে এই '$+$' আর '$\cdot$'-এর সঙ্গে সাধারণ যোগ আর গুণ গুলিয়ে যায়, তাই আমরা $\mathbb{Z}_n$-কে একটু অন্যভাবে লিখব--

We shall write $\mathbb{Z}_n = \{\overline{0}, \overline{1}, ..., \overline{n-1}\}$.

যেমন, যদি $\overline{1} + \overline{3}$ লিখি, তবে বুঝবে যে modulo n যোগ হচ্ছে। আর যদি $1 + 3$ লিখি তবে বুঝবে সাধারণ যোগ হচ্ছে।

If part:

Given: n is prime.

To show: $(\mathbb{Z}_n, +, \cdot)$ is an integral domain. We know from standard result that $(\mathbb{Z}_n, +, \cdot)$ is a commutative. ring with identity. So enough to show that it has no zero divisor, ie,

$$\forall \overline{a}, \overline{b} \in \mathbb{Z}_n \quad (\overline{a} \cdot \overline{b} = \overline{0} \implies \overline{a} = \overline{0} \text{ or } \overline{b} = \overline{0}).$$

অর্থাৎ কিনা দুটো জিনিসের গুণফল শূন্য হলে ওদের মধ্যে অন্ততঃ একজন শূন্য হতে বাধ্য।

$\forall a, b$

Take any $\overline{a}, \overline{b} \in \mathbb{Z}_n$ with $\overline{a} \cdot \overline{b} = \overline{0}$.

Then $n | ab$.

$\because n$ is prime, $\therefore$ either $n|a$ or $n|b$,

ie, either $\overline{a} = \overline{0}$ or $\overline{b} = \overline{0}$, as required.

Only if part:

Given: $(\mathbb{Z}_n, +, \cdot)$ is an integral domain.

To show: n must be a prime.

এখানে আমরা contradiction লাগাব।

Let, if possible, n be not a prime.

যদি $n \in \mathbb{Z}$ একটা prime সংখ্যা না হয়, তবে হয় $n = 1$ আর নয়তো n একটা composite সংখ্যা।

Case 1: $n = 1$: Then $\mathbb{Z}_n = \{\overline{0}\}$, and so the trivial ring ($\Rightarrow\Leftarrow \because$ integral domain is nontrivial by definition).

Case 2: n is composite: Let $n = ab$ where $a, b \in \{2, ..., n-1\}$

Then $\overline{a}, \overline{b} \neq \overline{0}$ in $\mathbb{Z}_n$.

But since $ab \equiv 0 (\text{mod } n)$, hence $\overline{a} \cdot \overline{b} = \overline{0}$.

Thus $\overline{a}$ and $\overline{b}$ are both zero divisors ($\Rightarrow\Leftarrow \because$ an integral domain cannot have zero divisors).

■

একটা ছোটো প্রয়োগ দেখি।

Example 48: True or false? Justify. The ring $\mathbb{Z}_6$ of all integers modulo 6 is an integral domain.[2] **(2009,2003,2005)**

SOLUTION:

The result is false, because $2 \times 3 = 6$, and so $2 \odot 3 = 0$, where $\odot$ is multiplication modulo 6.

Thus 2 and 3 are both zero divisors in $\mathbb{Z}_6$.

■

Example 49: Let R be a commutative ring with 1. Prove that R is an integral domain if and only if $\forall a, b, c \in R$ with $a \neq 0$, $ab = ac$ implies $b = c$. **(1997,2002,2007)**

SOLUTION:

Only if part:

Given: R is an integral domain.

To show

◎ $\forall a, b, c \in R \quad \big[(a \neq 0, \quad ab = ac) \implies b = c\big]$.

$\forall a, b, c$ Take any $a, b, c \in R$ with $a \neq 0$ and $ab = ac$.

Then $a(b-c) = ab - ac = 0$,
$\therefore b - c = 0$, since $a \neq 0$ and R has no zero divisor.
Thus, $b = c$, as required.

এইবার উল্টো দিকটা দেখাতে হবে।

If part:

To show R is an integral domain, ie,

- R is commutative (given),
- $1 \in R$ (given),
- R has no zero divisor (shall show)
- R is nontrivial (shall assume)

অংকটার এই দিকটায় একটু ভুল আছে। আমাদের যে শর্তটা দেওয়া আছে সেটা trivial ring-এর ক্ষেত্রেও খাটে (vacuously true)। কিন্তু trivial ring মোটেই একটা integral domain নয়। তাই আমরা অংকটাকে মেরামত করার জন্য ধরে নিয়েছি যে ring-টা nontrivial. তাহলে পড়ে থাকে খালি zero divisor নেই দেখানো--

To show that R has no zero divisor.
Let, if possible, $a, b \in R$ be such that $a, b \neq 0$ but $ab = 0$. Then $ab = 0 = a0$.
Hence by the given condition $b = 0 (\Rightarrow\Leftarrow$ since $b \neq 0)$.

■

Example 50: An element a of a ring R is called nilpotent if $a^n = 0$ for some integer $n \geq 1$.

Show that an integral domain has no nonzero nilpotent element.[2] **(2010.4cii)**
SOLUTION: একটা nilpotent-এর উদাহরণ এইরকম। ধরো এই matrix-টা

$$A = \begin{bmatrix} 0 & 1 & 2 \\ 0 & 0 & 3 \\ 0 & 0 & 0 \end{bmatrix}.$$

তাহলে A বা A^2 মোটেই zero matrix নয়, কিন্তু A^3-টা হবে zero matrix.

Let, if possible, an integral domain R contain a nonzero nilpotent element a.
Let $n \geq 1$ be the least integer such that $a^n = 0$.

এখানে $n \geq 2$ হবেই কারণ $a \neq 0$. আমাদের উদাহরণে $n = 3$ ছিল।

$\because a \neq 0, \therefore n \geq 2.$
Let $b = a^{n-1}$.
Then $b \neq 0$ (as n is the least integer ≥ 1 with $a^n = 0$).
Now $ab = a \cdot a^{n-1} = a^n = 0$.
So a is a zero divisor ($\Rightarrow\Leftarrow \because$ an integral domain cannot have zero divisors).

■

12.1 Characteristic

একটা ring দেওয়া থাকলে তার characteristic কাকে বলে সেটা আমরা এই অধ্যায়ে আগেই শিখেছি--সবচেয়ে ছোটো $n \in \mathbb{N}$, যাতে তুমি যাই $a \in R$ নাও না কেন,

$$\underbrace{a + \cdots + a}_{n \text{ বার}} = 0$$

হবে। যদি এরকম কোনো n না পাওয়া যায়, তবে characteristic বলব 0. এই সংজ্ঞাটার সমস্যা হল যাবতীয় $a \in R$ নিয়ে পরীক্ষা করে দেখতে হয়। কিন্তু যদি ring-টার মধ্যে unity থাকে তবে কাজটা অনেক সহজ হয়ে যায়, খালি $1 + \cdots + 1$ করে দেখলেই হয়। ফলে definition-টা দাঁড়ায় এরকম--

DEFINITION: **Characteristic of ring with unity**

If R is a ring with unity, 1, then its characteristic is defined as the least $n \in \mathbb{N}$ such that

$$\underbrace{1 + \cdots + 1}_{n \text{ times}} = 0.$$

The characteristic is defined to be 0, if no such $n \in \mathbb{N}$ exists.

যেহেতু integral domain-দের মধ্যে unity থাকে, তাই ওদের বেলায় এই সহজ definition-টা ব্যবহার করা যায়।

Example 51: $(\mathbb{Z}_3, \oplus, \otimes)$-এর characteristic কত হবে বলো তো?

SOLUTION: $1 \neq 0,\ 1 \oplus 1 \neq 0$, কিন্তু $1 \oplus 1 \oplus 1 = 0$. তাই $(\mathbb{Z}_3, \oplus, \otimes)$-এর characteristic হল 3. ■

Example 52: What is the characteristic of $(\mathbb{Z}, +, \bullet)$?[1] **(2008)**

SOLUTION:

Since in $\mathbb{Z}$ we have

$$\forall n \in \mathbb{N} \underbrace{1 + \cdots + 1}_{n \text{ times}} = n \neq 0,$$

so the characteristic of $\mathbb{Z}$ is 0.

■

■

Example 53: Prove that the characteristic of an integral domain is either zero or a prime.[3]

(1999,2001,2006,2008,2010)

SOLUTION: দেখাতে হবে যে, যেকোনো integral domain-এর characteristic হয় 0 নয়তো prime. এরকম "হয় এটা নয়তো ওটা"-জাতীয় অংক করার একটা কায়দা হল "এটা" নয় ধরে নিয়ে "ওটা" প্রমাণ করা। আমরা এখানে ধরে নেব characteristic-টা 0 নয়, এবং দেখাব যে, সেক্ষেত্রে characteristic-টা prime হতে বাধ্য।

> Let R be an integral domain with characteristic $n \neq 0$. To show that n must be prime.
> Let, if possible, n be not prime. Since R is nontrivial, so $n \neq 1$.
> So $n = pq$ where $1 < p, q < n$.

এখানে একটা সূক্ষ্ম প্যাঁচ আছে। একটা সংখ্যা $n \in \mathbb{N}$ যদি prime না হয়, তার মানেই যে composite হবে এমন নয়, $n = 1$-ও হতে পারে। এখানে $n = 1$ হতে পারে না কারণ ring-টা nontrivial. (Characteristic 1 হওয়া মানে $1 = 0$ অর্থাৎ trivial ring.)

> By definition of characteristic, n is the smallest positive integer such that
> $$\underbrace{1 + \cdots + 1}_{n \text{ times}} = 0. \qquad (*)$$
> Let $\overline{n} = \underbrace{1 + \cdots + 1}_{n \text{ times}}$.

এখানে $\overline{n}$ লিখেছি, কারণ যোগটা হচ্ছে R-র মধ্যে। সুতরাং n-খানা 1 যোগ করলে n নাও হতে পারে। যেমন $\mathbb{Z}_5$-এর মধ্যে 7-টা 1 যোগ করলে 2 হয়।

> Simularly, let
> $$\overline{p} = \underbrace{1 + \cdots + 1}_{p \text{ times}}$$
> $$\overline{q} = \underbrace{1 + \cdots + 1}_{q \text{ times}}$$
> Then $\overline{n} = 0$, but $\overline{p} \neq 0$ and $\overline{q} \neq 0$.
> Since $\overline{pq} = \overline{n} = 0$,
> so $\overline{p}$ and $\overline{q}$ must be zero divisors ($\Rightarrow\Leftarrow \because R$ is an integral domain).

■

Integral domain-দের characteristic আমরা দেখলাম *nonzero* হলেই prime হতে বাধ্য। কিন্তু এর উল্টো দিকটাও কী ঠিক? মানে একটা ring (ধরো commutative, আর unity-ও আছে), যদি তার characteristic একটা prime সংখ্যা হয়, তা হলেই কী সেটা একটা integral domain হবেই? সেটা যে নয়, তা নিয়েই এবারের অংকটা।

Example 54: Give an example of a commutative ring with unity which contains divisors of zero and whose characteristic is prime. Justify your answer.[3] **(2010.5aii)**

SOLUTION:

> Consider the ring $R = \{(m,n) \ : \ m,n \in \mathbb{Z}_2\}$, where addition and multiplication are defined as
>
> $$\begin{aligned}(a,b) \oplus (m,n) &= (a \oplus_2 m, b \oplus_2 n),\\ (a,b) \otimes (m,n) &= (a \otimes_2 m, b \otimes_2 n).\end{aligned}$$
>
> Here $\oplus_2$ and $\otimes_2$ are addition and multiplication, respectively, modulo 2.
>
> This is a commutative ring because $(\mathbb{Z}_2, \oplus_2, \otimes_2)$ is a commutative ring.
>
> This ring has unity $(1,1)$ where 1 is the unity of $\mathbb{Z}_2$.
>
> This ring has characteristic 2 (a prime), because
>
> $$(1,1) \neq (0,0) \text{ but } (1,1) \oplus (1,1) = (0,0).$$
>
> Also R has divisors of zero, because $(1,0) \otimes (0,1) = (0,0)$ though $(1,0), (0,1) \neq (0,0)$.
>
> So both $(1,0)$ and $(0,1)$ are divisors of zero.

■

DAY 13
Field (part 1)

আমাদের যাত্রা শুরু হয়েছিল group থেকে। তারপর এল ring, সেখান থেকে integral domain. এর উপর যদি আরও একটা শর্ত চাপাই, তবে পাব আরেকটা নতুন abstract structure, যার নাম **field.** এক লাইনে লিখতে হলে field-এর সংজ্ঞা হল--এমন একটা integral domain, যেখানে প্রতিটি nonzero element-এরই multiplicative inverse আছে। বা বলা যায়, প্রতিটি nonzero element-ই হল unit. এই কথাটাকেই আমরা একটু গুছিয়ে লিখব (integral domain ব্যবহার না করে)--

> DEFINITION: **Field**
>
> A **field** is a non-trivial commutative ring with unity where every nonzero element is a unit.

Field-এর সবচেয়ে পরিচিত উদাহরণ হল $(\mathbb{R}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$ এবং $(\mathbb{C}, +, \cdot)$.

13.1 Field দেখানো

এবার আমরা কয়েকটা অংক করব যেখানে একটা set দেওয়া থাকবে R, এবং তার উপর একটা addition আর multiplication দেওয়া থাকবে। আমাদের পরীক্ষা করে দেখতে হবে সব মিলিয়ে একটা field হয় কিনা। আমরা দেখেছি যে, ring দেখানোই যথেষ্ট ঝঞ্ঝাটের, একরাশ শর্ত পরীক্ষা করতে হয়। আর field দেখানো মানে ring-এর যাবতীয় শর্ত তো আছেই, তার উপরে আরও তিনটে শর্ত--

1. R is commutative, অর্থাৎ multiplication-টা commutative. (আর addition-টা তো commutative ছিলই)। তার মানে দেখাতে হবে $\forall a, b \in R \quad ab = ba$.

2. R has multiplicative identity, মানে $1 \in R$.

3. Every nonzero element has inverse. মানে যে কোনো nonzero element-এর multiplicative inverse থাকবে R-এর মধ্যেই, অর্থাৎ

$$\forall a (\neq 0) \in R \quad \exists b \in R \quad ab = ba = 1.$$

   এখানে b-কে বলব a^{-1}. লক্ষ কর যে, commutativity-র সুবাদে আমাদের $ab = 1$ দেখালেই চলবে, আলাদা করে $ba = 1$ দেখাতে হবে না।

আগেই বলেছি যে, একেবারে শুরু থেকে field প্রমাণ করা বেশ লম্বা কাজ। কিন্তু যদি একটা ring-কে field দেখাতে হয়, তবে কাজটা অনেক সহজ, কারণ সেক্ষেত্রে খালি উপরের তিনটে শর্ত পরীক্ষা করলেই চলে, যেহেতু ring অবধি দেওয়াই আছে।

Example 55: $\mathbb{C}$ denotes the set of complex numbers. Does the ring $(\mathbb{C}, +, \bullet)$ under the usual addition and multiplication form a field? **(2004)**

SOLUTION:

Yes, it forms a field.

Since $(\mathbb{C}, +, \bullet)$ is already given to be a ring, enough to show that

1. it is commutative,
2. it has multiplicative identity,
3. nonzero elements have multiplicative inverses.

Step 1: Commutative:

For any two $a + b\mathbf{i}, c + d\mathbf{i} \in \mathbb{C}$ (with $a, b, c, d \in \mathbb{R}$) we have

$$(a + b\mathbf{i}) \bullet (c + d\mathbf{i}) = (ac - bd) + (ad + bc)\mathbf{i} = (c + d\mathbf{i}) \bullet (a + b\mathbf{i}).$$

Step 2: Multiplicative identity:

$1 + 0\mathbf{i} \in \mathbb{C}$ is the multiplicative identity, since for any $a + b\mathbf{i} \in \mathbb{C}$ (with $a, b \in \mathbb{R}$) we have

$$(a + b\mathbf{i}) \bullet (1 + 0\mathbf{i}) = (1 + 0\mathbf{i}) \bullet (a + b\mathbf{i}) = (a + b\mathbf{i}).$$

Step 3: Multiplicative inverse: To show: $\forall z \in \mathbb{C}$ if $z \neq 0$ then $\exists y \in \mathbb{C}$ such that $y \bullet z = z \bullet y = 1$.

Take any $z \neq 0$ in $\mathbb{C}$. Let $z = a + \mathbf{i}b$. Since $z \neq 0$, at least one of a and b is nonzero.

Define

$$y = \frac{a}{a^2+b^2} - \mathbf{i}\frac{b}{a^2+b^2} \in \mathbb{C},$$

which is well-defined since at least one of a and b is nonzero.

এটা কোথা থেকে পেলাম। আমরা হায়ার সেকণ্ডারীতে $\frac{1}{a+\mathbf{i}b}$-র উপর নীচে $a - \mathbf{i}b$ গুণ করে লেখার কায়দা শিখেছিলাম, মনে আছে। এখানে আসলে সেটাই করেছি।

Then

$$y \bullet z = z \bullet y = \left[\frac{a}{a^2+b^2} - \mathbf{i}\frac{b}{a^2+b^2}\right](a+\mathbf{i}b) = 1,$$

as required.

Thus, $(\mathbb{C}, +, \bullet)$ is a field.

■

Example 56: Prove that the ring of matrices

$$\left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} | a, b \in \mathbb{R} \right\}$$

is a field. **(2000)**

SOLUTION:

Let R be the given ring. To show that R is a field it is enough to show the following.

Step 1: R is commutative:

Take any

$$A = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}, \quad B = \begin{bmatrix} p & q \\ -q & p \end{bmatrix} \in R.$$

Then

$$AB = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}\begin{bmatrix} p & q \\ -q & p \end{bmatrix} = \begin{bmatrix} ap-bq & aq+bp \\ -aq-bp & ap-bq \end{bmatrix},$$

and

$$BA = \begin{bmatrix} p & q \\ -q & p \end{bmatrix}\begin{bmatrix} a & b \\ -b & a \end{bmatrix} = \begin{bmatrix} ap-bq & aq+bp \\ -aq-bp & ap-bq \end{bmatrix} = AB.$$

So $\forall A, B \in R$ we have $AB = BA$.

> Step 2: R has multiplicative identity: Taking $a = 1$, and $b = 0$,
>
> $$\begin{bmatrix} a & b \\ -b & a \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in R.$$
>
> Step 3: Each nonzero element has inverse: Let
>
> $$\begin{bmatrix} a & b \\ -b & a \end{bmatrix} \in R$$
>
> be nonzero, ie, at least one of a, b is nonzero. Then its determinant is $a^2 + b^2 \neq 0$. So the matrix is nonsingular with inverse
>
> $$\frac{1}{a^2+b^2}\begin{bmatrix} a & -b \\ b & a \end{bmatrix},$$
>
> which is of the form $\begin{bmatrix} p & q \\ -q & p \end{bmatrix}$ for
>
> $$p = \frac{a}{a^2+b^2} \text{ and } q = \frac{-b}{a^2+b^2}.$$
>
> Thus the inverse is in R, as required.

■

Example 57: Let $(F, +, \bullet)$ be a field and $u(\neq 0) \in F$. Define multiplication $\times$ in F as $a \times b = a \bullet u \bullet b$ for $a, b \in F$. Prove that $(F, +, \times)$ is a field.[5] **(2008)**

SOLUTION: লক্ষ কর যে $(F, +, \times)$ আর $(F, +, \bullet)$-এর '+'-টুকু একই। সুতরাং addition-ঘটিত শর্তগুলো আর নতুন করে দেখাতে হবে না। খালি multiplication-ঘটিত শর্তগুলো দেখালেই চলবে--

> $(F, +, \times)$ inherits all additive properties from $(F, +, \bullet)$.
>
> Shall prove the multiplicative properties:
>
> Associative:
>
> $\forall a, b, c \in F$
>
> $$\begin{aligned} (a \times b) \times c &= (a \bullet u \bullet b) \bullet u \bullet c \\ &= a \bullet u \bullet (b \bullet u \bullet c) \quad [\text{ by associativity of } \bullet] \\ &= a \times (b \times c). \end{aligned}$$
>
> Commutative:

$\forall a, b \in F$

$$\begin{aligned}(a \times b) &= (a \bullet u \bullet b) \\ &= (b \bullet u \bullet a) \quad [\text{ by commutativity of } \bullet] \\ &= b \times a.\end{aligned}$$

Distributive:

$\forall a, b, c \in F$

$$\begin{aligned}a \times (b + c) &= a \bullet u \bullet (b + c) \\ &= a \bullet u \bullet b + a \bullet u \bullet c \quad [\text{ by distributivity of } \bullet \text{ over } +] \\ &= a \times b + a \times c.\end{aligned}$$

Distributive law-র আবার দুটো দিক আছে, একটা দিক তো দেখানো হল, এবার উল্টো দিকটা commutativity থেকেই চলে আসবে--

By commutativity, we also have $(b + c) \times a = b \times a + c \times a$.

আমরা ছোটোবেলা থেকে যেটাকে 1 বলে ভাবতে অভ্যস্ত, multiplicative identity-টা যে সবসময়ে ঠিক সেটাই হবে এমন নয়। এখানেই আমরা তার একটা উদাহরণ দেখব।

Multiplicative identity:

$\because u \neq 0 \ \therefore u^{-1} \in F$.

u^{-1} is the multiplicative identity, because $\forall a \in F$

$$a \times u^{-1} = a \bullet u \bullet u^{-1} = a \bullet 1 = a.$$

Also, by commutativity, $u^{-1} \times a = a$.

Multiplicative inverse:

For nonzero $a \in F$ the multiplicative inverse is $a^{-1} \bullet u^{-2}$,

এখানে u^{-2} মানে হল $(u^{-1})^2$. একটু ভেবে নিই এখানে ঠিক কী দেখাতে হবে। আমরা দেখাবো যে, a আর $a \bullet u^{-2}$-কে গুণ (মানে $\times$) করলে পাব $(F, +, \times)$-এর multiplicative identity, মানে u^{-1} (সাবধান, 1 নয় কিন্তু!)।

because

$$a \times (a^{-1} \bullet u^{-2}) = a \bullet u \bullet a^{-1} \bullet u^{-2} = u^{-1},$$

which is the multiplicative identity in $(F, +, \times)$.

Similarly, by commutativity, $(a^{-1} \bullet u^{-2}) \times a = u^{-1}$.

So $(F, +, \times)$ is indeed a field, as required.

■

Example 58: Prove that the set F of all matrices of the form

$$\begin{bmatrix} a & b \\ 2b & a \end{bmatrix}$$

forms a field w.r.t. the usual matrix addition and matrix multiplication where $a, b \in \mathbb{Q}$. Is the result true if $a, b \in \mathbb{R}$? **(1998,2003,2007)**

SOLUTION: এই অংকটায় আমাদের দেখাতে হবে F একটা field. মুস্কিল হল, field-এর সংজ্ঞায় অনেকগুলো শর্ত আছে, সবগুলো মিলিয়ে দেখতে অনেক সময় লাগবে। আমরা যথাসম্ভব সংক্ষেপে কাজ সারতে চাই। তাই একটা কাছাকাছি জানা কিছু থেকে শুরু করব। আমরা জানি যে, $M_2(\mathbb{Q})$ অর্থাৎ rational সংখ্যা দিয়ে তৈরী যাবতীয় 2×2 matrix-এর set-টা একটা ring. এইখান থেকে শুরু করলে অনেকটা পরিশ্রম বাঁচানো যাবে। প্রথমে দেখাব F হল $M_2(\mathbb{Q})$-র একটা subring. তাতেই প্রমাণ হয়ে যাবে যে F একটা ring. আর ring থেকে field-এ পৌঁছতে দেখাতে হবে খালি তিনটে জিনিস-- F-এর মধ্যে multiplication হচ্ছে commutative, F-এ multiplicative identity আছে আর F-টা closed under multiplicative inverse.

> We know that the set $M_2(\mathbb{Q})$ of all 2×2 matrices with rational entries forms a ring under usual matrix addition and multiplication.
>
> Shall first show that F is a ring, by showing that F is a subring of $M_2(\mathbb{Q})$.

Subring দেখানোর যথারীতি তিনটে ধাপ--

> Step 1: Nonempty: $F \neq \phi$, since taking $a = b = 0$,
>
> $$\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \in F.$$
>
> Steps 2,3: Closure under difference and multiplication:
>
> Let $\begin{bmatrix} a & b \\ 2b & a \end{bmatrix}, \begin{bmatrix} p & q \\ 2q & p \end{bmatrix} \in F.$
>
> Then $a, b, p, q \in \mathbb{Q}$, and so
>
> $$\begin{bmatrix} a & b \\ 2b & a \end{bmatrix} - \begin{bmatrix} p & q \\ 2q & p \end{bmatrix} = \begin{bmatrix} a-p & b-q \\ 2(b-q) & a-p \end{bmatrix} \in F,$$
>
> since $a-p, b-q \in \mathbb{Q}$.
>
> Also
>
> $$\begin{bmatrix} a & b \\ 2b & a \end{bmatrix}\begin{bmatrix} p & q \\ 2q & p \end{bmatrix} = \begin{bmatrix} ap+2bq & aq+bp \\ 2(aq+bp) & ap+2bq \end{bmatrix} \in F,$$
>
> since $ap+2bq, aq+bp \in \mathbb{Q}$.
>
> So F is a subring of $M_2(\mathbb{Q})$, and hence a ring.

এবার field দেখানোর পালা।

> Next we shall show that the ring F is a field.
>
> Step 4: Multiplication is commutative:
>
> $$\begin{bmatrix} a & b \\ 2b & a \end{bmatrix} \begin{bmatrix} p & q \\ 2q & p \end{bmatrix} = \begin{bmatrix} ap+2bq & aq+bp \\ 2(aq+bp) & ap+2bq \end{bmatrix}$$
>
> and
>
> $$\begin{bmatrix} p & q \\ 2q & p \end{bmatrix} \begin{bmatrix} a & b \\ 2b & a \end{bmatrix} = \begin{bmatrix} ap+2bq & aq+bp \\ 2(aq+bp) & ap+2bq \end{bmatrix},$$
>
> same as above.
>
> Step 5: Multiplication has identity: Taking $a = 1, b = 0$ we get the identity matrix.
>
> Step 6: Closure under inverse:
>
> Let $\begin{bmatrix} a & b \\ 2b & a \end{bmatrix} \in F$ be a nonzero matrix.
>
> Then $a, b \in \mathbb{Q}$ and at least one of them is nonzero.
>
> Then
>
> $$\begin{bmatrix} a & b \\ 2b & a \end{bmatrix}^{-1} = \frac{1}{a^2 - 2b^2} \begin{bmatrix} a & -b \\ -2b & a \end{bmatrix} \in F,$$
>
> since $a^2 - 2b^2 \in \mathbb{Q}$ and $a^2 - 2b^2 \neq 0$, because otherwise $\sqrt{2}$ becomes a rational number.
>
> So F is indeed a field, as required.

এবার দেখব যে $a, b \in \mathbb{R}$ হলেও field হবে কি না। লক্ষ কর আমরা যখন $a, b \in \mathbb{Q}$ নিয়ে কাজ করছিলাম, তখন matrix -টা invert করতে গিয়ে দেখাতে হয়েছিল যে, determinant-টা, মানে $a^2 - 2b^2$, কখনও শূন্য হতে পারে না। কিন্তু a, b যদি যে কোনো real number হতে পারে, তবে তো সেই সুবিধা আর থাকছে না, যেমন $a = \sqrt{2}$ আর $b = 1$ নিলেই $a^2 - 2b^2 = 0$ হয়ে যাবে। সুতরাং তখন আর matrix-টাকে invert করা যাবে না। অতএব--

> No, the set is not a field if $a, b \in \mathbb{R}$.
>
> For example, taking $a = \sqrt{2}$ and $b = 1$, the matrix
>
> $$\begin{bmatrix} \sqrt{2} & 1 \\ 2 & \sqrt{2} \end{bmatrix}$$
>
> has determinant 0, and so is not invertible.

■

Example 59:

$$M = \left\{ \begin{bmatrix} a & b \\ 3b & a \end{bmatrix} : a, b \in \mathbb{Q} \right\}.$$

If + and • denote matrix addition and multiplication, respectively, then show that the ring $(M, +, \bullet)$ is a field, but not a field if $a, b \in \mathbb{R}$.[4+1] **(2007)**
SOLUTION: এই অংকটা ঠিক আগেরটার মতই। তাই আর নতুন করে করলাম না। ■

Example 60: Prove that the ring of matrices

$$\left\{ \begin{bmatrix} a & b \\ 3b & a \end{bmatrix} \; : \; a, b \in \mathbb{Q} \right\}$$

forms a field under matrix addition and matrix multiplication, where $\mathbb{Q}$ is the set of rational numbers.[3] **(2009.5ai)**
SOLUTION: আগের অংকটাই, সামান্য অন্য ভাষায়। ■

Example 61: Let S denote the set of all functions $f : \mathbb{R} \to \mathbb{R}$. Define '+' and '*' on S by

$$(f + g)(a) = f(a) + g(a) \text{ and } (f * g)(a) = f(a)g(a)$$

for all $a \in \mathbb{R}$ and for all $f, g \in S$. Assuming S to be a commutative ring with identity, check if this is a field. **(2001)**
SOLUTION:

> No, this is not a field, as it has zero divisors. For example,
>
> $$f(x) = \begin{cases} 1 & \text{if } x \leq 0 \\ 0 & \text{otherwise} \end{cases} \quad \text{and } g(x) = \begin{cases} 0 & \text{if } x \leq 0 \\ 1 & \text{otherwise} \end{cases}$$
>
> are both nonzero functions, but $g * f = 0$.

এমনটা হবার কারণ এই যে, f যেখানে nonzero, সেসব জায়গায় g-টা zero. আবার g-টা যে সব জায়গায় nonzero, সেখানে f-টা zero. ■

DAY 14
Field (part 2)

14.1 Integral domain-এর সঙ্গে field-এর সম্পর্ক

Example 62: Prove that every field is an integral domain.[2] **(2008,2010.5ci)**

SOLUTION: আমরা field-এর সংজ্ঞা থেকে জানি যে, এটা একটা nontrivial, commutative ring with unity, যার মধ্যে সব nonzero element-ই হল একেকটা unit. সুতরাং integral domain-এর প্রায় সব শর্তই সংজ্ঞার মধ্যেই ধরা আছে। খালি integral domain-এর মধ্যে কোনো zero divisor থাকা চলবে না, সেটুকু দেখাতে হবে।

Let F be a field. Then by definition it is a commutative ring with unity. To show that it is an integral domain, it is enough to show that it has no zero divisor, ie,

$\forall a, b \in F \quad (ab = 0 \implies (a = 0$ or $b = 0))$.

$\forall a, b$ Take any $a, b \in F$ such that $ab = 0$.

এখানে দেখাতে হবে হয় $a = 0$ নয়তো $b = 0$. এরকম "হয় এটা নয়তো ওটা"-জাতীয় জিনিস প্রমাণ করার সময়ে সাধারণতঃ "এটা" নয় ধরে "ওটা" প্রমাণ করা হয়--

Let $a \neq 0$. Shall show that $b = 0$.
Since a is a nonzero element in a field, so $a^{-1} \in F$.
Hence multiplying both sides of $ab = 0$ with a^{-1} we have $a^{-1}ab = a^{-1}0$, or $1b = 0$, or $b = 0$, as required.

■

Example 63: True or false? Justify. Every field is an integral domain. **(2001)**

SOLUTION: আগের অংকটাই। ■

Example 64: Prove that a field does not contain divisor of zero.[3] **(2009.4ci)**

SOLUTION: আগের অংকটার মতই। ■

Example 65: True or false? Justify. There does not exist divisors of zero in a field F.[2] **(1998)**

SOLUTION: আগের অংকটাই। ■

Example 66: Give an example of a field that is a finite integral domain.[1] **(2007)**

SOLUTION: যেকোনো finite field-এর উদাহরণ দিলেই চলবে। তা, সবচেয়ে বাচ্চা finite field-টাই দেওয়া যাক--

$(\mathbb{Z}_2, \oplus, \odot)$ is a field that is a finite integral domain. Here $\oplus$ and $\odot$ denote, respectively, addition and multiplication modulo 2.

■

এতক্ষণ দেখলাম যে, field মানেই integral domain হতে বাধ্য। এর উল্টোটাও কি সত্যি? না[2]। সেটাই নীচের অংকটার বক্তব্য।

[2] নইলে কি আর লোকে সাধ করে দুটো আলাদা নাম field এবং integral domain ব্যবহার করে!

Example 67: Give an example of an integral domain which is not a field.[1] **(2008)**

SOLUTION:

> $(\mathbb{Z}, +, \cdot)$ is an integral domain, but not field.
>
> It is not a field because $2(\neq 0)$, for example, has no multiplicative inverse in $\mathbb{Z}$ ($\because \frac{1}{2} \notin \mathbb{Z}$).

■

এবার আমরা কয়েকটা অত্যন্ত গুরুত্বপূর্ণ অংক দেখব যেখানে আমরা finite set-এর এই বৈশিষ্ট্যটা ব্যবহার করব--

> যদি A একটা finite set হয়, আর $f : A \to A$ হয় যে কোনো একটা function, তবে f-এর পক্ষে one-one হওয়া, onto হওয়া এবং bijective হওয়া সমার্থক।

এই জিনিসটা আমরা প্রথম অধ্যায়ে প্রমাণ করেছিলাম।

Example 68: Prove that a finite integral domain is a field. Is the converse true? Justify your answer. **(1998,2000,2002,2004,2005,2007)**

SOLUTION:

> Let R be a finite integral domain.
>
> Shall show that it is a field.

Integral domain-এর সংজ্ঞায় field-এর প্রায় সব শর্তই ধরা আছে। বাকি আছে খালি একটাই-- সব nonzero element-ই unit হবে। এটুকু দেখিয়ে দিলেই হবে--

> To show that
>
> ◎ $\forall a(\neq 0) \in R \quad \exists b \in R \quad ab = ba = 1.$
>
> $\forall a$ Take any $a(\neq 0) \in R$.
>
> Define $f : R \to R$ as $f(x) = ax$.
>
> This function is one-one because
>
> $$f(x) = f(y) \implies ax = ay \implies a(x - y) = 0 \implies x - y = 0,$$
>
> since R has no zero divisor and $a \neq 0$.

এবার finite set-এর সেই বৈশিষ্ট্যটা কাজে লাগাব--

> Since R is finite, this means f is also onto.
>
> So $\exists b \in R$ such that $f(b) = 1$.
>
> $\exists b$ Choose this $b \in R$.
>
> Then, by commutativity, $ba = ab = f(b) = 1$, as required.

■

এবার দ্বিতীয় অংশ--

> The converse is: All fields are finite integral domains.
>
> This is not true.
>
> For example, $\mathbb{R}$ is a field that is not finite.
>
> However, all fields are integral domains.

■

Example 69: Prove that a finite integral domain is a field.[5] **(2012.4,2009.5b)**

SOLUTION: আগের অংকেই করা হয়েছে। ■

এবার একটা অংক করব, যেটা অনেকটা একইরকম, কিন্তু তাও কিছুটা অন্য স্বাদের।

Example 70: Prove that every nonzero element in a finite ring having no divisor of zero is a unit. Does the theorem hold if the ring contains an infinite number of elements? Justify your answer.[4+1] **(2008)**

SOLUTION: চট্ করে দেখলে মনে হতে পারে যে, এটা বস্তুতঃ আগের অংকটাই আরেকবার। কিন্তু তা নয়। এখানে আমরা integral domain থেকে শুরু করছি না। তাই এখানে আমাদের unity-র অস্তিত্ব দেখাতে হবে। তাছাড়া commutativity দেওয়া নেই, তাই unity দেখানোর জন্য $1a = a$ এবং $a1 = a$ আলাদা করে দেখাতে হবে। একইভাবে unit দেখানোর জন্য $aa^{-1} = 1$ এবং $a^{-1}a = 1$-ও আলাদা করে দেখাতে হবে। ফলে সমাধানটা অনিবার্যভাবেই লম্বা হবে!

> First part:
>
> If R is trivial, then it has no nonzero element, and hence the result is vacuously true.
>
> Step 1: Shall show that R has unity.
>
> Substep 1.1: Cancellation laws hold in R:
>
> If $a, b, c \in R$ with $a \neq 0$ and $ab = ac$, then $a(b - c) = 0$.
>
> Since R has no zero divisor, so $b - c = 0$, or $b = c$.
>
> Similarly, if $ba = ca$, then also we have $b = c$.
>
> Substep 1.2:
>
> We pick any $a(\neq 0) \in R$.
>
> Let $f : R \to R$ be defined as $f(x) = ax$.
>
> Then f is one-one.
>
> ⟦ Because:
>
> $f(x) = f(y) \implies ax = ay \implies x = y$, by cancellation law.
>
> ⟧

Since R is finite, f is also onto.
So $\exists e \in R$ such that $f(e) = a$, or

$$ae = a. \qquad (*)$$

এবার ধাপে ধাপে দেখাব যে, এই e-টা সত্যিই multiplicative identity. আমরা এখনও পর্যন্ত খালি দেখিয়েছি যে কেবল একটা বিশেষ a-র ক্ষেত্রে $ae = a$ হয়। এবার দেখাব যে সেই বিশেষ a-টার জন্য $ea = a$-ও হয়। তারপরের ধাপে দেখাব যে যেকোনো $r \in R$-এর জন্যই $re = er = r$ হয়।

Substep 1.3: Shall show $ea = a$: Multiplying $(*)$ by a from right, we have $aea = a^2$, or, by left-cancellation,

$$ea = a. \qquad (**)$$

Substep 1.4: Shall show that

$$\forall r \in R \quad er = re = r.$$

Take any $r \in R$.
Multiplying $(*)$ from right by r, we have $aer = ar$, or $er = r$ by left-cancellation of a.
Similarly, from $(**)$ we get $re = r$.
Thus e is the multiplicative identity of R.
We shall call it $1 \in R$.

এই অব্‌ধি গেল unity-র অস্তিত্ব দেখানো। এটা না দেখালে unit দেখানো অসম্ভব।

Step 2: Shall show

◎ $\forall b (\neq 0) \in R \quad \exists c \in R \quad bc = cb = 1.$

$\forall b$ Take any $b(\neq 0) \in R$.
We define a function $g : R \to R$ as $g(x) = bx$.
Then, arguing like substep 1.2, g is one-one and hence onto.
So $\exists c \in R$ such that $g(c) = 1$,
$\exists c$ Choose this $c \in R$.
Then $bc = f(c) = 1$.

এবার দেখাতে হবে যে $cb = 1$ হবে। মনে রেখো যে R-কে commutative দেওয়া নেই, সুতরাং এখানে অল্প একটু খাটতে হবে--

> Also $cb = 1$,
>
> ⟦ <u>Because:</u>
>
> Since $bc = 1$, so multiplying by b from right, $bcb = b1$,
> and cancelling b from left, $cb = 1$.
>
> ⟧
>
> This completes the proof.

এবার পরের অংশ, যেখানে আমরা infinite ring নিয়ে মাথা ঘামাব।

> <u>Second part:</u>
>
> No, the result fails for infinite rings.
>
> For example $(\mathbb{Z}, +, \cdot)$ is an infinite ring without zero divisors, but $2(\neq 0)$ is not a unit $(\because \frac{1}{2} \notin \mathbb{Z})$.

■

Example 71: True or false? Justify. Any finite ring with unity is a field. **(2003)**

SOLUTION:

> The result is not true. For example, $(\mathbb{Z}_6, \oplus, \odot)$ is a finite ring where $\oplus$ and $\odot$ are addition and multiplication, respectively, modulo 6, but it is not a field, because it has zero divisors: $2 \odot 3 = 0$ but $2, 3 \neq 0$.

■

14.2 Prime order fields

এবার এক ধরণের অতি গুরুত্বপূর্ণ field-এর কথা শিখব, যাদের বলে **prime order field**. এরা একধরণের field যাদের সাইজ হল prime. সেই CD, DVD আর Galois theory-র গল্প বলেছিলাম, সেখানে এইরকম field-এর প্রচুর প্রয়োগ।

Example 72: If n is a positive prime number then prove that the ring $\mathbb{Z}_n$ of all integers modulo n is a field. Is the converse true? Justify your answer. **(1998,2005)**

SOLUTION:

প্রথমে একটা prime n নিয়ে শুরু করি--

> Let n be a positive prime.

সরাসরি $(\mathbb{Z}_n, \oplus, \odot)$-কে একটা field দেখানো সহজ কাজ নয়, তাতে অনেক কিছু লিখতে হবে। আমরা তাই একটা শর্ট-কাট নেব--

> We know that any finite integral domain is a field. So enough to show that $(\mathbb{Z}_n, \oplus, \odot)$ is a finite integral domain.
>
> We already know that $(\mathbb{Z}_n, \oplus, \odot)$ is a finite, nontrivial, commutative ring with 1. Shall show that it has no zero divisor.

এখানে nontrivial বললাম কারণ n যেহেতু একটা prime positive integer তাই $n > 1$. তার মানে ring-টায় অন্ততঃ দুটো element আছেই।
এবার proof by contradiction.

> Let, if possible, $a, b \in \mathbb{Z}_n$ such that $a, b \neq 0$ but $a \odot b = 0$.
>
> This means $n|ab$.
>
> But since n is a prime, either $n|a$ or $n|b$. But it is not possible, since $0 < a, b < n (\Rightarrow\Leftarrow)$.

এবার উল্টোদিকটা ঠিক কিনা দেখতে হবে, মানে $(\mathbb{Z}_n, \oplus, \odot)$ যদি field হয়, তবে n-টা prime হতে বাধ্য কিনা।

> The converse is true.

সেটাকেই সামান্য ঘুরিয়ে লিখলে হয়--

> ie, if $n \in \mathbb{N}$ is not prime, then $(\mathbb{Z}_n, \oplus, \odot)$ cannot be a field.

যদি $n \in \mathbb{N}$-টা prime না হয়, তবে হয় $n = 1$ নয়তো n একটা composite number.

> If $n = 1$ then $\mathbb{Z}_n = \mathbb{Z}_1$ is the trivial ring, and hence not a field.
>
> Otherwise, n is composite, and we can factorise it as $n = pq$ where $0 < p, q < n$. Then $p, q \in \mathbb{Z}_n,\ p, q \neq 0$, but $p \odot q = 0$.
>
> So $\mathbb{Z}_n$ has zero divisor, and hence cannot be a field.

■

Example 73: True or false? Justify. A subring with identity of a field is an integral domain.[2]

(2000)

SOLUTION:

> The result is true, directly from definition,

একটু বিশদ করা যাক--

> because the subring has 1 by assumption, inherits commutativity from the field, and has no zero divisor, since a field has no zero divisor.

■

DAY 15
Field (part 3)

15.1 Subfield

Subgroup কাকে বলে শিখেছো, subring-ও শিখেছো। সুতরাং **subfield**-এর সংজ্ঞা কী হবে আন্দাজ করতেই পারছ।

Example 74: Define subfield of a field. **(1999,2001,2005)**

SOLUTION:

> DEFINITION: **Subfield**
>
> Let $(F, +, \bullet)$ be a field. Then $S \subseteq F$ is called a **subfield** if $(S, +, \bullet)$ is again a field.

■

একটা উদাহরণ এইরকম--$(\mathbb{R}, +, \bullet)$ একটা field, তার একটা subfield হল $(\mathbb{Q}, +, \bullet)$.
যেহেতু subfield এবং মূল field-টার যোগ আর গুণ একই, ফলে subfield দেখানোর জন্য অনেক কিছুই আর নতুন করে করতে হয় না, সেগুলো মূল field-টার থেকে উত্তরাধিকারসূত্রে পাওয়া যায়। নতুন করে দেখাতে হয় খালি তিনটে শর্ত। যদি F হয় মূল field-টা, আর আমাদের দেখাতে বলা হয় যে $S \subseteq F$ তার একটা subfield তবে এই তিনটে শর্ত হল--

1. $S \neq \phi$,
2. Closure under difference, মানে $a, b \in S$ হলে $a - b \in S$ হতে হবে।
3. Closure under ratio, মানে $a, b \in S$ এবং $b \neq 0$ হলে $ab^{-1} \in S$ হবে।

Example 75: Show that the set

$$A = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$$

is a subfield of $\mathbb{R}$. **(1999,2001,2005)**

SOLUTION:

<u>Nonempty:</u>

$S \neq \phi$ because $0 = 0 + 0\sqrt{2} \in S$.

<u>Closure under difference:</u> Take any $a + b\sqrt{2},\ c + d\sqrt{2} \in A$ for $a, b, c, d \in \mathbb{Q}$.

Then $(a + b\sqrt{2}) - (c + d\sqrt{2}) = (a - c) + (b - d)\sqrt{2} \in A$, because $a - c,\ b - d \in \mathbb{Q}$.

<u>Closure under ratio:</u>

> Let $a+b\sqrt{2}, c+d\sqrt{2} \in A$ with $a,b,c,d \in \mathbb{Q}$ and $c+d\sqrt{2} \neq 0$. So and at least one of c,d is nonzero.

দেখাব যে

$$\frac{a+b\sqrt{2}}{c+d\sqrt{2}} \in A.$$

এর জন্য আমরা ছোটোবেলায় যে "করণী নিরসন" শিখেছিলাম (ইংরাজীতে করণীকে বলে surd), সেটা লাগাব।

> Then
> $$\frac{a+b\sqrt{2}}{c+d\sqrt{2}} = \frac{a+b\sqrt{2}}{c+d\sqrt{2}} \cdot \frac{c-d\sqrt{2}}{c-d\sqrt{2}} = \frac{(ac-2bd)+(bc-ad)\sqrt{2}}{c^2-2d^2},$$
> which is in A, since
> $$\frac{ac-2bd}{c^2-2d^2}, \frac{bc-ad}{c^2-2d^2} \in \mathbb{Q},$$
> because $c,d \neq 0$ and $\sqrt{2}$ is irrational.

■

Example 76: Show that the set

$$S = \{a+b\sqrt{5} \;:\; a,b \in \mathbb{Q}\}$$

is a subfield of the field of real numbers $\mathbb{R}$.[3] **(2012.5b)**
SOLUTION: আগের অংকের মতই। ■

Example 77: True or false? Justify. If

$$\mathbb{Q}[\sqrt{2}] = \{a+b\sqrt{2} \mid a,b \in \mathbb{Q}\}$$

then the ring $(\mathbb{Q}[\sqrt{2}],+,\bullet)$ is a field.[2] **(2005,2007)**
SOLUTION: এখানে ওই $\mathbb{Q}[\sqrt{2}]$ জিনিসটা দেখে ঘাবড়ে যেও না, ওটা একটা notation মাত্র। চাইলে তুমি মনে মনে ওর জায়গায় অন্য কোনো notation, যেমন F বা R কল্পনা করে নিতে পারো। তাতে কিচ্ছু বদলাবে না।

> The statement is true.

Ring থেকে শুরু করে field পর্যন্ত প্রমাণ করা যায়, কিন্তু আমরা একটু খাট্‌নি বাঁচাব এইভাবে--

> We have $\mathbb{Q}[\sqrt{2}] \subseteq \mathbb{R}$. So enough to show that $\mathbb{Q}[\sqrt{2}]$ is a subfield of $\mathbb{R}$.

এখন field-এর অনেক শর্তই $\mathbb{R}$ থেকে উত্তরাধিকারসূত্রে পাব, সেগুলো আর নতুন করে দেখাতে হবে না। দেখাতে হবে খালি তিনটে জিনিস। কী করে সেই তিনটে জিনিস দেখাতে হয়, সেটা তো Example 75-এই বিশদভাবে বলা হয়েছে, তাই সেই অংকটার উত্তর এর নীচে জুড়ে দিলেই এবার চলবে। ■

আমরা দেখেছিলাম যে, group-এর identity আর subgroup-এর identity একই হয়। কিন্তু subring-এর বেলায় unity নিয়ে সমস্যা বাঁধে। Ring-এর unity-র থাকা বা না থাকার সঙ্গে subring-এর unity-র বলতে গেলে কোনোই সম্পর্ক নেই। নীচের অংকটা অভয় দিচ্ছে যে, field-এর বেলায় আর সে সমস্যা নেই। দ্বিতীয় অধ্যায়ে group-এর জন্য যেভাবে করেছিলাম, প্রমাণটা একেবারে সেভাবে করে গেলেই অনায়াসে হবে।

Exercise 13: Let F be a field and S be any subfield. Then show that the unity of S must be the same as the unity of F. ■

Example 78: In the field $\mathbb{R}$ of all real numbers, show that the set

$$A = \{a + b\sqrt{3} : a, b \in \mathbb{Q}\}$$

is a subfield, but the set

$$B = \{b\sqrt{3} : b \in \mathbb{Q}\}$$

is not. **(1997)**

SOLUTION: প্রথম অংশটা Example 75-এর মতই। দ্বিতীয় অংশটার সমাধান এইরকম--

> Let, if possible, B be a subfield of $\mathbb{R}$. Then the unity if B must the unity of $\mathbb{R}$.
> So $1 \in B$.
> But 1 cannot be written as $b\sqrt{3}$ for $b \in \mathbb{Q}$ $(\Rightarrow\Leftarrow \because \sqrt{3} \notin \mathbb{Q})$.
> Hence B cannot be a field.

■

Example 79: Let $S = \{a + b\sqrt{5} : a, b \in \mathbb{R}\}$. Prove that S is a commutative ring with 1 under usual addition and multiplication. Is this a field? Justify your answer.[5] **(2006)**

SOLUTION:

> Actually $S = \mathbb{R}$.
>
> ⟦ <u>Because:</u>
> Clearly, $S \subseteq \mathbb{R}$.
> Also $\mathbb{R} \subseteq S$, because
> $\forall x \in \mathbb{R}$ we have $x = x + 0\sqrt{5} \in S$.
> ⟧

S যদি $\mathbb{R}$-ই হয়ে গেল, তো আর বাকী রইল কি? আমরা জানি যে $\mathbb{R}$ একটা commutative ring with 1, এবং একটা field-ও বটে। সুতরাং S-ও এই সবই!

> So S is a commutative ring with 1 under usual addition and multiplication.
>
> Also S is a field.

∎

∎

Example 80: True of false: If $\mathbb{R}(\sqrt{3}) = \{a + b\sqrt{3} : a, b \in \mathbb{R}\}$ then the ring $(\mathbb{R}(\sqrt{3}), +, \bullet)$ is a field.[2] **(2004)**

SOLUTION: এখানেও আগের অংকের মতই $\mathbb{R}(\sqrt{3})$ আসলে $\mathbb{R}$ নিজেই! ∎

যেকোনো field-এর মধ্যেই কী অন্ততঃ একটা subfield থাকবেই? উত্তর হল--হ্যাঁ, কারণ field-টা তো নিজেই নিজের একটা subfield. যদি সেই কেসটাকে বাদ দিই, তবে যে সব subfield পড়ে থাকে, তাদের বলে **proper subfield.** সেরকম subfield কিন্তু সব সময়ে নাও থাকতে পারে। নীচের অংকেই তার একটা উদাহরণ আছে।

Example 81: Show that $\mathbb{Q}$ has no proper subfield. **(2006)**

SOLUTION:

> Let, if possible, $\mathbb{Q}$ have a proper subfield F.

যেহেতু F হল $\mathbb{Q}$-এর একটা proper subset তাই F-টা পুরো $\mathbb{Q}$ নয়। সুতরাং আমরা এমন একটা rational number পাব $\frac{p}{q}$ যেটা F-এর মধ্যে নেই।

> Pick any $\frac{p}{q} \notin F$, where $p, q \in \mathbb{Z}$ with $q \neq 0$.

এখানে $\frac{p}{q}$ সংখ্যাটা positive বা negative দুই-ই হতে পারে। বলাই বাহুল্য যে positive-এর জন্য করা গেলে negative-এর জন্যও একইভাবে করা যাবে। তাই positive আর negative এই দুটো case-কে আলাদা করে না করে খালি positive-এর জন্যই করব।

> Assume, without loss of generality, that $p, q > 0$.

এখানে "without loss of generality" বলার তাৎপর্য এই যে, অন্য case-টা (মানে negative-এর case-টা) একইভাবে হবে।

আমরা এবার দেখাতে চলেছি $\frac{p}{q} \in F$, কারণ তাহলেই একটা contradiction পাব, যেহেতু $\frac{p}{q} \notin F$ ধরে শুরু করেছিলাম। $\frac{p}{q} \in F$ কথাটা আমরা ধাপে ধাপে দেখাব, প্রথমে দেখাব $p, q \in F$, তারপর দেখাব $\frac{1}{q} \in F$, এবং তা থেকে দেখাব যে $\frac{p}{q} = p \times \frac{1}{q} \in F$.

> Since F is a subfield of $\mathbb{Q}$, so $1 \in F$. So
>
> $$p = \underbrace{1 + \cdots + 1}_{p \text{ times}} \in F,$$
>
> and
>
> $$q = \underbrace{1 + \cdots + 1}_{q \text{ times}} \in F,$$
>
> since F is closed under addition.
>
> Also, since F is closed under multiplicative inverse, and $q \neq 0$,

So

$$\frac{1}{q} \in F.$$

Since F is closed under multiplication, so

$$\frac{p}{q} = p \times \frac{1}{q} \in F (\Rightarrow\Leftarrow \because \frac{p}{q} \notin F).$$

Hence $\mathbb{Q}$ has no proper subfield.

■

Example 82: Show that the field $\mathbb{Q}$ of rational numbers has no proper subfield.[3] **(2010.5cii)**

SOLUTION: আগের অংকটাই। ■

Example 83: Prove or disprove: The field $(\mathbb{Q}, +, \bullet)$ of rationals has no proper subfield.[3] **(2009.5cii)**

SOLUTION: আগের অংকেই করা হয়েছে। ■

15.2 Equations

Field-এর মধ্যে equation solve করা খুব সোজা, ঠিক যেমন স্কুলে করতাম সেরকম। এমনি সংখ্যা দিয়ে যেমন যোগ, বিয়োগ, গুণ, ভাগ করা চলে, যেকোনো field-এও সেসবই করা যায় একই ভাবে। (তা বলে ফূর্তির চোটে 0 দিয়ে ভাগ করে বোসো না যেন!)

Example 84: True or false? Justify. In a field F the equation $ax = b$ has a unique solution where $a, b \in F$ and $a \neq 0$. **(2002,2006)**

SOLUTION:

The result is true.

মনে রেখো যে, এখানে দুটো জিনিস দেখাতে হবে--প্রথমতঃ, equation-টার solution আছে, এবং দ্বিতীয়তঃ, ঠিক একটাই solution আছে। আমরা এই দুটো কাজই একসঙ্গে সেরে দেব--

The given equation is $ax = b$. Since $a \neq 0$, so a^{-1} exists.

Now

$$\begin{aligned} & ax = b \\ \iff & a^{-1}ax = a^{-1}b \\ \iff & x = a^{-1}b. \end{aligned}$$

> So $x = a^{-1}b$ is the unique solution, as required.

এখানে unique ব্যাপারটা কোথা থেকে পেলাম? আসলে $\iff$ -এর দুটো অংশ $\implies$ আর $\impliedby$. এর মধ্যে $\impliedby$ -টার জন্য $x = a^{-1}b$ হল একটা solution, অর্থাৎ যদি $x = a^{-1}b$ হয়, তবে $ax = b$ হবে। আর $\implies$ -টা বলছে যে, যদি $ax = b$ হয় তবে $x = a^{-1}b$ না হয়ে যায় না, অর্থাৎ unique solution.

■

নীচের অংকটাও একইরকম। সমাধানটা দেখে নেবার আগে, নিজে করার চেষ্টা করো।

Example 85: Let F be a field. If $a, b, c \in F$ with $a \neq 0$, then show that the equation $ax + b = c$ has a unique solution in F.[2] **(2008)**

SOLUTION:

> Take any $a, b, c \in F$ with $a \neq 0$.
>
> Then $a^{-1} \in F$.
>
> Now
>
> $$\begin{aligned} ax + b = c &\iff ax = c - b \\ &\iff a^{-1}ax = a^{-1}(c - b) \\ &\iff x = a^{-1}(c - b). \end{aligned}$$
>
> So $x = a^{-1}(c - b)$ is the unique solution, as required.

■

Example 86: In a field F if $a^2 - b^2 = 0$, then show that either $a = b$ or $a = -b$. **(2003,2005)**

SOLUTION:

> In a field
>
> $$(a^2 - b^2) = (a + b)(a - b).$$
>
> So the given condition is
>
> $$(a + b)(a - b) = 0.$$
>
> Since a field does not have any zero divisor, this means
>
> $$\text{either } a + b = 0 \text{ or } a - b = 0,$$
>
> ie,
>
> $$\text{either } a = -b \text{ or } a = b,$$
>
> as required.

■

Example 87: True or false? Justify. Let F be a field. If $a, b \in F$ such that $b \neq 0$ and $(ab)^2 = ab^2 + bab - b^2$ then $a = 1$. **(2003)**

SOLUTION:

> The result is true.
>
> Given
> $$(ab)^2 = ab^2 + bab - b^2,$$
> or, using commutativity of multiplication,
> $$a^2b^2 = 2ab^2 - b^2 = (2a-1)b^2.$$
> Since $b \neq 0$, we can cancel b^2 from both sides to get
> $$a^2 = 2a - 1,$$
> or
> $$a^2 - 2a + 1 = 0,$$
> or
> $$(a-1)^2 = 0.$$
> Since a field has no zero divisor this means $a - 1 = 0$, ie, $a = 1$, as required.

■

Example 88: True or false? Justify. In a field F, $(-a)^{-1} = -(a^{-1})$ for all $a \in F$, $a \neq 0$. **(2005)**

SOLUTION: একটা উদাহরণ মাথায় রাখলে সুবিধা হবে। ধরো $F = \mathbb{R}$ আর $a = 2$. তাহলে নিশ্চয়ই সন্দেহ নেই যে, $\frac{1}{-2} = -\frac{1}{2}$? এবং 2 জায়গায় যেকোনো nonzero সংখ্যা নিলেও একইরকম ব্যাপার হত। সুতরাং আন্দাজ করা যাচ্ছে যে--

> The statement is true.

অবশ্য খালি $\mathbb{R}$ নিয়ে কাজ করলেই চলবে না। আমাদের কাজ করতে হবে যেকোনো field নিয়ে, এবং দেখাতে হবে

$$(-a)^{-1} = -(a^{-1}),$$

অর্থাৎ $-(a^{-1})$ হল $(-a)$-র multiplicative inverse. তার মানে এটা দেখালেই হবে যে $-(a^{-1})$ আর $(-a)$-কে গুণ করলে 1 হয়। যেহেতু field-এর multiplication commutative, তাই গুণের সময়ে কে আগে কে পরে থাকছে তাতে কিছু এসে যায় না।

> $(-a)(-(a^{-1}))$
> $= (-1a)[-1(a^{-1})]$
> $= (-1)(-1)aa^{-1}$ [by associativity and commutativity of multiplication.]
> $= 1.$

So

$$(-a)^{-1} = -(a^{-1}),$$

as required.

■

Example 89: True or false? Justify. The field $(\mathbb{Z}_3, +, \bullet)$ is of characteristic 3. **(2006)**

SOLUTION:

The result is true, because in $(\mathbb{Z}_3, +, \bullet)$

$$1 \neq 0, \quad 1+1=2 \neq 0, \quad 1+1+1=0.$$

লক্ষ কর যে এখানে খালি $1+1+1=0$ লিখে ছেড়ে দিলেই চলত না। আমাদের এটাও দেখানো দরকার যে তিনটের চেয়ে কমসংখ্যক 1 যোগ করলে 0 পাওয়া যায় না। সেই কারণেই $1 \neq 0$ আর $1+1 \neq 0$ লিখতে হয়েছে। ■

Example 90: True or false? Justify. There exists a field with 7 elements. **(2001)**

SOLUTION:

The result is true. $(\mathbb{Z}_7, \oplus, \odot)$ is a field with 7 elements $0, 1, 2, 3, 4, 5, 6$, where $\oplus$ and $\odot$ denote addition and multiplication, respectively, modulo 7.

এখানে অবশ্যই 7-কাহন করে লিখতে বসব না, কেন $\mathbb{Z}_7$ একটা field, খালি সংক্ষেপে লিখে দেব--

$\because 7$ is a prime,

$\therefore (\mathbb{Z}_7, \oplus, \odot)$ is an integral domain.

Also it is finite.

Since every finite integral domain is a field,

so $(\mathbb{Z}_7, \oplus, \odot)$ is a field.

■

Answers

1. **(1)** ভুল, unity নিজে তো অন্ততঃ একটা unit. **(2)** ঠিক। **(3)** ভুল, $\mathbb{Z}$-এর মধ্যে -1 একটা unit কিন্তু সেটা unity নয়। **2.** হ্যাঁ, সম্ভব। $R = 2\mathbb{Z} \times \mathbb{Z}$-এর কোনো unity নেই, কিন্তু $S = \{0\} \times \mathbb{Z}$-এর মধ্যে দিব্যি unity আছে-- $(0, 1)$. **3.** আগের অংকের উত্তরে $\mathbb{Z}$-এর জায়গায় $M_2(\mathbb{Z})$ বসিয়ে দাও। **4.** A, B দুজনেই subring হলে $0 \in A$ এবং $0 \in B$. সুতরাং $0 \in A \cap B$, তাই $A \cap B \neq \phi$. আবার যদি $x, y \in A \cap B$ হয়, x, y দুজনেই A-তেও আছে, B-তেও আছে, তাই $x - y$ আর xy-ও A, B দুজনের মধ্যেই আছে। সুতরাং $x - y, xy \in A \cap B$. **5.** না, ring-টায় unity আছে কিনা বলে দেয়নি। **7.** প্রথমে তুমি যে কোনো $x \in R$ নিয়েছ। একথা ঠিক যে $xe = x$. কিন্তু কি করে জানলে যে e-টা এখানে unique? অংকে বলা ছিল যে unique e আছে যাতে $\forall x \in R \quad xe = x$ হয়। কিন্তু একটা

বিশেষ x-এর জন্য একাধিক e যে থাকবে না এমন কিছু তো বলা নেই! **10.** $1 + bxa$ হবে $1 - ba$-র multiplicative inverse. **11.** $\because gcd(m, n) = 1,\ \therefore \exists a, b \in \mathbb{Z} \quad am + bn = 1$. এবার দুইপাশকে n দিয়ে ভাগ করে ভাগশেষ নাও, $\bar{a}\bar{m} = 1$. এখানে $\bar{a}$ হল a-র ভাগশেষ, আর $\bar{m}$ হল m-এর ভাগশেষ। সুতরাং $\bar{a}$ হচ্ছে $\bar{m}$-এর multiplicative inverse, তাই $\bar{m}$ হল একটা unit. **12.** $1, 5, 7, 11$. **13.** ধরো F-এর unity হল 1_F, আর S-এর unity হল 1_S. তাহলে $1_S 1_F = 1_S$ এবং $1_S 1_S = 1_S$. সুতরাং $1_S 1_S = 1_S 1_F$. এবার বাঁদিক থেকে 1_S কেটে নিলেই হবে।

Chapter V
Group theory (3rd yr)

DAY 1
Isomorphism এবং homomorphism

1.1 কুমীরছানার গল্প

বলতে পারো এমন কতগুলো group সম্ভব, যাদের মধ্যে ঠিক একটাই element আছে? যে কোনো group-এই identity তো থাকবেই, সুতরাং একমাত্র element-টা নিশ্চয়ই identity-টাই হবে। সুতরাং এরকম একটা group হল $(\{0\},+)$. এখানে $0+0=0$. কিন্তু এটাই কি একমাত্র উদাহরণ? না, আরেকটা উদাহরণ হল $(\{1\},\times)$. এখানে $1\times 1=1$. একটু চিন্তা করলেই বুঝবে যে, দুটো উদাহরণ আসলে একই--খালি 0-র জায়গায় 1 আর $+$-এর জায়গায় $\times$ লিখেছি মাত্র। সুতরাং এটা খালি চিহ্নের হেরফের। বস্তুতঃ এরকম চিহ্নের হেরফের করে যত খুশী group বানানো যায়, যেমন ধরো set-টা নিলাম {চেয়ার}. এখানে তুমি চেয়ার, টেবিল, $a,b,c,d,$ যা খুশী নিতে পারো! আর binary operation-টা নিলাম $\star$ যার সংজ্ঞা হল

চেয়ার $\star$ চেয়ার $=$ চেয়ার।

তাহলে অবশ্যই ({চেয়ার}, $\star$) একটা group হবে, যেটা আগের group দুটোরই নামান্তর।
এই যে তিনটে group দেখলাম--

$(\{0\},+)$, $(\{1\},\times)$ আর ({চেয়ার}, $\star$),

বুঝতেই পারছ যে এরা কাঠামোর দিক দিয়ে একই group, পার্থক্য কেবল বহিরঙ্গে। এদের অংকের ভাষায় বলে **isomorphic** (আইসোমর্ফিক)। "Iso" মানে একইরকম, আর "morph" মানে হল চেহারা বা কাঠামো। তাই isomorphic মানে দাঁড়ালো--একইরকম কাঠামোবিশিষ্ট। অনেক সময়ে আমরা এইভাবেও বলি--"there is a group isomorphism between $(\{0\},+)$ and $(\{1\},\times)$. " একটু চিন্তা করলেই বুঝবে যে, কোনো group-এর সাইজ যদি 1 হয়, তবে সেটার পক্ষে অন্য কোনোরকম কাঠামো হওয়া অসম্ভব। তাই আমরা বলে থাকি যে "there is only one group of size 1 up to isomorphism." ওই যে "up to isomorphism" লিখেছি, তার মানে এখানে কাঠামোটাই গুরুত্বপূর্ণ, দুটো group-এর কাঠামো এক হলে ওদের আমরা আলাদা করে গুণছি না।
এই প্রসঙ্গে ছোটোবেলায় পড়া একটা গল্প মনে পড়ল--একটা কুমীর তার সাত ছানাকে শেয়াল পণ্ডিতের কাছে পড়াশোনা করতে পাঠিয়েছিল। শেয়ালটা একদিন লোভে পড়ে ছয়টা ছানাকে খেয়ে ফেলেছে। এবার তো কুমীর এসেছে পেরেন্ট্-টিচার মিটিং-এ, এসে বলছে আমার সাত ছানা কই? শেয়াল গম্ভীরভাবে বলল, দাঁড়ান, সবাইকে তো এক সঙ্গে আনা যাবে না, সেটা আমাদের স্কুলের ডিসিপ্লিন-সম্মত নয়, তাই একজন একজন করে আনতে হবে। বলে ওই একটা অবশিষ্ট ছানাকেই সাত বার একেকবার একেকরকম করে সাজিয়ে এনে দেখিয়ে দিল। কুমীরের চোখ খারাপ ছিল বোধহয়, বুঝতে না পেরে খুশী হয়ে চলে গেল।
তুমি হয়তো ভাবছ এটা একেবারে বাজে গল্প, একই ছানাকে বার বার দেখাল আর কুমীরটা চিনতে পারল না? আসলে কুমীরের দোষ নেই, group-এর বেলাতেও দেখবে isomorphic group-দের চোখে দেখে অনেক সময়েই isomorphic বলে চেনা কঠিন। একটা উদাহরণ দিই।

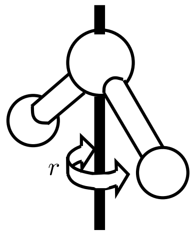


Fig 1

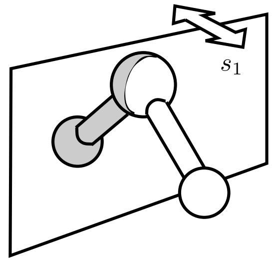


Fig 2

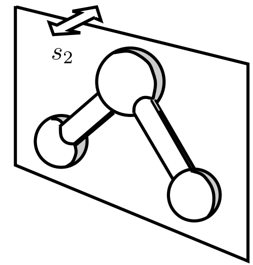


Fig 3

Example 1: আমরা power set-এর উপর symmetric difference-কে binary operation করে group বানিয়েছিলাম মনে আছে? যদি set-টা নিই $\{0, 1\}$ তবে তার power set হবে--

$$\{\ \phi,\ \{0\},\ \{1\},\ \{0,1\}\ \}.$$

এর উপরে symmetric difference দিয়ে group বানালে পাব Klein's 4-group (K_4).
এবার জলের molecule-এর symmetry group-টার কথা ভাবো। সেটা ছিল এইরকম--

$$\{e, r, s_1, s_2\}.$$

Fig 1, Fig 2 আর Fig 3 দেখে মনে করে নাও r, s_1 আর s_2 কী ছিল। বললে কি বিশ্বাস হবে যে, এই দুটো group আসলে একই, মানে isomorphic?

SOLUTION: বিশ্বাস হওয়া শক্ত। দুটো group-এর নামতাই পাশাপাশি দিলাম। ভালো করে দ্যাখো--যদি বাঁদিকের টেবিলের ϕ-এর জায়গায় e বসাও, $\{0\}$-এর জায়গায় r, $\{1\}$-এর জায়গায় s_1, আর $\{0,1\}$-এর জায়গায় s_2, তবেই ডানদিকের টেবিলটা পাওয়া যায়!

Power set group

	ϕ	$\{0\}$	$\{1\}$	$\{0,1\}$
ϕ	ϕ	$\{0\}$	$\{1\}$	$\{0,1\}$
$\{0\}$	$\{0\}$	ϕ	$\{0,1\}$	$\{1\}$
$\{1\}$	$\{1\}$	$\{0,1\}$	ϕ	$\{0\}$
$\{0,1\}$	$\{0,1\}$	$\{1\}$	$\{0\}$	ϕ

Water molecule group

	e	r	s_1	s_2
e	e	r	s_1	s_2
r	r	e	s_2	s_1
s_1	s_1	s_2	e	r
s_2	s_2	s_1	r	e

তার মানে দুটো group-এর কাঠামো একই, অর্থাৎ ওরা isomorphic. ■

যেহেতু দুটো group-ই আসলে এক, তাই Klein's 4-group বলতে এদের যে কোনোটাকেই বোঝানো যায়। তাই এটা বলাই ভালো যে, Klein's 4-group বা K_4 হল আসলে এই কাঠামোটার নাম। এই একই কাঠামো ব্যবহার করে আরেকটা অংক দিচ্ছি।

Exercise 1: $(\mathbb{Z}_2, \oplus)$ বলে একটা group-এর কথা শিখেছিলাম, মনে আছে নিশ্চয়ই। এর set-টা ছিল $\{0, 1\}$ আর binary operation-টা ছিল modulo 2 addition, মানে এমনি যোগ করে 2 দিয়ে ভাগ করে ভাগশেষ নেওয়া। এই group-টাকে ব্যবহার করে একটা নতুন group বানাব এইভাবে--set-টা নেব $\mathbb{Z}_2 \times \mathbb{Z}_2$, মানে

$$\{\ (0,0),\ (0,1),\ (1,0),\ (1,1)\ \}.$$

এর উপর binary operation-টা হবে $\star$ যেখানে

$$(a, b) \star (c, d) = (a \oplus c, b \oplus d).$$

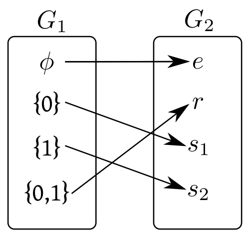


Fig 4

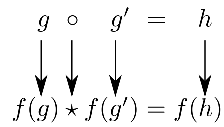


Fig 5

মানে (a, b) আর (c, d)-র প্রথম দুটো সংখ্যা a আর c-এর উপরে $\oplus$ লাগাচ্ছি, আবার পরের দুটোর উপর আলাদা করে $\oplus$ লাগাচ্ছি। একটু চিন্তা করলেই বুঝবে যে, $(\mathbb{Z}_2 \times \mathbb{Z}_2, \star)$ সত্যিই একটা group হচ্ছে। দেখাতে পারো যে, এটাও আসলে Klein's 4-group-এরই আরেকটা ছদ্মবেশ? ■

দুটো group G_1 আর G_2-কে isomorphic দেখাতে হলে G_1-এর কোন element-এর জায়গায় G_2-র কোন element বসালে হিসেব মিলবে, সেটা বোঝা সব সময়ে সহজ নয়। বস্তুতঃ এই কাজটা একাধিকভাবে করেও হিসেব মিলিয়ে দেওয়া যায়। যেমন ধরো এক্ষুণি যে power set আর জলের molecule-এর অংকটা করলাম, সেখানে আমরা এইভাবেও এগোতে পারতাম--

ϕ-এর জায়গায় e, $\{0\}$-র জায়গায় s_1, $\{1\}$-এর জায়গায় s_2, আর $\{0, 1\}$-এর জায়গায় r.

Exercise 2: অন্য কোনোভাবে কাজটা করা যায়? ■

এই যে আমরা G_1-এর একেকটা element-এর জায়গায় G_2-র একেকটা element বসালাম, এটাকে Fig 4-এর মত লাইন টেনে জোড় বেঁধে দেখানো যায়। বুঝতেই পারছ যে, এইভাবে জোড় বাঁধার সময়ে কাউকে বাদ দিয়ে যাওয়া চলবে না, এবং কোনো group-এর একটা element-কে কখনও অন্য group-এর একাধিক element-এর সঙ্গে জোড় বাঁধা চলবে না। অর্থাৎ অংকের ভাষায় এই জোড় বাঁধাটা হল একটা one-one এবং onto function, বা এক কথায় একটা bijection. অবশ্য যে কোনো bijection নিলেই হবে না, সেটা যেন group দুটোর binary operation-এর সঙ্গে সামঞ্জস্যপূর্ণ থাকে (Fig 5), মানে যদি G_1 আর G_2-র binary operation দুটোকে যথাক্রমে $\circ$ আর $\star$ লিখি, আর $f : G_1 \to G_2$ একটা isomorphism হয়, তবে আমরা চাই

$$\forall g, g' \in G_1 \quad f(g \circ g') = f(g) \star f(g').$$

এ থেকেই আসে নীচের সংজ্ঞাটা--

DEFINITION: **Group isomorphism**

Let $(G_1, \circ)$ and $(G_2, \star)$ be two groups. Then a function $f : G_1 \to G_2$ is called a **group isomorphism** if

1. f is a bijection, and
2. $\forall g, g' \in G \quad f(g \circ g') = f(g) \star f(g')$.

Example 2: আমরা জানি যে $(\mathbb{R},+)$ আর $(\mathbb{R}_+,\times)$ হল দুটো group. এখানে $\mathbb{R}_+$ মানে যাবতীয় $positive, realnumber$-এর set. দেখাও যে $f:\mathbb{R}\to\mathbb{R}_+$ যদি এরকম নিই--

$$f(x)=e^x$$

তবে f হল একটা isomorphism.

SOLUTION: আমরা জানি যে, e^x একটা one-one এবং $ontofunction$. আবার যদি $x,y\in\mathbb{R}$ নিই, তবে $f(x+y)=e^{x+y}=e^x\times e^y=f(x)\times f(y)$. সুতরাং f একটা isomorphism. ■

এই সংজ্ঞাটা দেখতে যতই সহজ বা কঠিন লাগুক, isomorphism ব্যাপারটাকে মনে রাখবে কুমীরছানার গল্পের মত করে। দুটো group যদি isomorphic হয় তার মানে ওরা আসলে একই group, খালি চিহ্নগুলো হয়তো অন্যরকমভাবে লেখা। সুতরাং প্রথম group-টার যাবতীয় বৈশিষ্ট্য দ্বিতীয়টাতেও থাকবে। যদি এরকম একটাও বৈশিষ্ট্যে দুটো group-এর মধ্যে অমিল পাও, তবে ওরা কোনোভাবেই পরস্পরের সঙ্গে isomorphic হতে পারে না। একটা উদাহরণ দেখি।

Example 3: দেখাও যে $(\mathbb{R}\setminus\{0\},\times)$ এবং $(\mathbb{R},+)$ পরস্পরের সঙ্গে isomorphic নয়। এখানে প্রথম group-টা তৈরী হয়েছে যাবতীয় nonzero, real number-দের নিয়ে।

SOLUTION: আমাদের কাজ হল একটা group-এর মধ্যে এমন কোনো বৈশিষ্ট্য বার করা যেটা অন্যটায় নেই। এরকম বৈশিষ্ট্য খুঁজে পাওয়া সব সময়ে সহজ হয় না। এখানে $(\mathbb{R}\setminus\{0\},\times)$-এর মধ্যে -1-কে লক্ষ কর। এটার order হল 2. (কারণ, $-1\neq 1$ এবং $(-1)^2=1$)। সুতরাং isomorphic হতে হলে $(\mathbb{R},0)$-র মধ্যেও এরকম একটা element থাকতে হবে। যদি x এরকম একটা element হয়, তবে আমরা চাই $x\neq 0$ কিন্তু $x+x=0$. বুঝতেই পারছ যে সেটা অসম্ভব! ■

Exercise 3: নীচের প্রতি ক্ষেত্রে এক জোড়া group দেওয়া হয়েছে। বলতে হবে কোন কোন ক্ষেত্রে ওরা isomorphic:

1. $K_4,\quad \mathbb{Z}_4$
2. $\mathbb{Z}_{24},\quad \mathbb{Z}_{40}$
3. $\mathbb{Z},\quad 2\mathbb{Z}$

■

Isomorphism হল এমন একটা function যার দুটো বৈশিষ্ট্য-- এক, ওটা একটা bijection, আর দুই ওটা group দুটো binary operation-এর মধ্যে সামঞ্জস্য রক্ষা করে চলে। যে সব function-এর এই দ্বিতীয় গুণটা আছে (প্রথমটা থাক বা না থাক), তাদের বলে **group homomorphism**. অংকের ভাষায় সংজ্ঞাটা নীচে দিলাম।

DEFINITION: **Group homomorphism**

Let $(G_1,\circ),(G_2,\star)$ be two groups. Then a function $f:G_1\to G_2$ is called a **group homomorphism** if

$$\forall a,b\in G_1\quad f(a\circ b)=f(a)\star f(b).$$

যদি একটা homomorphism আবার one-one এবং onto-ও হয়, তবে তাকে যে isomorphism বলে তা তো বলেইছি। এরকম আরও দুটো term আছে--

DEFINITION: Monomorphism, epimorphism

A **monomorphism** is a homomorphism that is one-one. An **epimorphism** is a homomorphism that is onto.

যে কোনো homomorphism-এরই দুটো দরকারী গুণ আছে--এক, ওরা একটা group-এর identity-কে অন্য group-টার identity-তে নিয়ে গিয়ে ফেলে, এবং inverse-কেও inverse-এ নিয়ে যায়। এটাই বলা হয়েছে নীচের theorem-টায়।

THEOREM

Let $(G_1, \circ), (G_2, \star)$ be two groups. Let $f : G_1 \to G_2$ be a group homomorphism. Then

1. $f(e_1) = e_2$, where e_1, e_2 are identity elements of G_1, G_2, respectively.
2. $\forall a \in G_1 \quad f(a^{-1}) = (f(a))^{-1}$.

Proof:

1. We have $e_1 \circ e_1 = e_1$.
So $f(e_1 \circ e_1) = f(e_1)$,
or, since f is a homomorphism, $f(e_1) \star f(e_1) = f(e_1)$.
Multiplying both sides by $\big(f(e_1)\big)^{-1}$, $f(e_1) = e_2$, as required.

এবার inverse-টা দেখাব--

2. To show
$\forall a \in G_1 \quad f(a) \star f(a^{-1}) = e_2 = f(a^{-1}) \star f(a)$.
Take any $a \in G_1$.
Then

$$\begin{aligned} f(a) \star f(a^{-1}) &= f(a \circ a^{-1}) \\ &= f(e_1) \\ &= e_2. \end{aligned}$$

Similarly,

$$\begin{aligned} f(a^{-1}) \star f(a) &= f(a^{-1} \circ a) \\ &= f(e_1) \\ &= e_2. \end{aligned}$$

[Q.E.D]

1.2 Image আর kernel

যে কোনো homomorphism-এর সঙ্গেই দুটো গুরুত্বপূর্ণ subgroup জড়িত থাকে, একটাকে বলে **image** (বা **range**), আর অন্যটাকে বলে **kernel**. এবার এদের কথা শেখা যাক।

> DEFINITION: **Image**
>
> Let $(G_1, \circ), (G_2, \star)$ be two groups. Let $f : G_1 \to G_2$ be a group homomorphism. Then its **image** or **range** is defined as
>
> $$Im(f) = \{f(x) \ : \ x \in G_1\}.$$

বস্তুতঃ এই সংজ্ঞাটার মধ্যে নতুন কিছু নেই, যেকোনো function-এর image বা range-এরই একই সংজ্ঞা, homomorphism-এর জন্য আলাদা কিছু নয়। একটা ছোট্টো অংক করে সংজ্ঞাটা হজম করে নেওয়া যাক।

Example 4: এই homomorphism-টা নাও--

$$f : (\mathbb{Z}, +) \to (\mathbb{Z}, +),$$

যেখানে $f(n) = 2n$. বল তো, 3 কি $Im(f)$-এর ভিতরে নাকি বাইরে?
SOLUTION: বাইরে, কারণ 3 একটা odd সংখ্যা, তাই ওকে $2n$ আকারে লেখা যায় না, অর্থাৎ $f(n)$ আকারে লেখা যায় না। সুতরাং $3 \notin Im(f)$. এখানে $Im(f)$ হল যাবতীয় even সংখ্যার set. ■

আগেই বলেছি, homomorphism-দের image-রা সবসময়ে subgroup হয়। নীচের অংকে ঠিক সেটাই দেখাতে বলেছে।

Example 5: $(G, \circ)$ and $(G', \star)$ are two groups and $\phi : (G, \circ) \to (G', \star)$ is a homomorphism. Prove that $Im(\phi)$ is a subgroup of $(G', \star)$.[3] **(2010.4b)**
SOLUTION: আমরা জানি যে, একটা group-এর কোনো subset-কে একটা subgroup দেখানোর জন্য দুইধাপে এগোনো যায়। প্রথমে দেখাতে হয় যে subset-টা nonempty. আর দ্বিতীয় ধাপে দেখাতে হয়, a, b যদি ওই subset-এ থাকে তবে $a^{-1}b$-ও ওই subset-এর মধ্যেই থাকবে।

Let e, e' be the identity elements of G, G', respectively.
$\because \phi$ is a group homomorphism, $\therefore e' = \phi(e)$.
$\therefore e' \in Im(\phi)$. So $Im(\phi) \neq \phi$.

এই গেল প্রথম ধাপ। এবার দ্বিতীয় ধাপ--

Shall show
$\forall a, b \in Im(\phi) \quad a^{-1} \star b \in Im(\phi)$.
$\forall a, b$ Take any $a, b \in Im(\phi)$.
Then $a = \phi(\alpha)$ and $b = \phi(\beta)$ for some $\alpha, \beta \in G$.

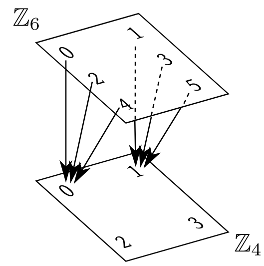


Fig 6

So

$$\begin{aligned} a \star b^{-1} &= \phi(\alpha) \star (\phi(\beta))^{-1} \\ &= \phi(\alpha) \star \phi(\beta^{-1}) \quad [\because \phi \text{ is homomorphism}] \\ &= \phi(\alpha \circ \beta^{-1}) \quad [\because \phi \text{ is homomorphism}]. \end{aligned}$$

But $\alpha \circ \beta^{-1} \in G$.

Hence $a \star b^{-1} \in Im(\phi)$.

So $Im(\phi)$ is a subgroup of G', as required.

■

Exercise 4: আমরা এই অংকে $(\mathbb{Z}_6, \oplus)$ থেকে $(\mathbb{Z}_4, \oplus)$-এ একটা homomorphism নেব $\phi(x) = x(\text{mod } 2)$, মানে x-কে 2 দিয়ে ভাগ করে ভাগশেষ নেওয়া। Fig 6 দ্যাখো। বল তো-- $Im(\phi)$ কি? ■

Image-এর কথা শিখলাম। এবার kernel-এর কথা শিখি। আবার Fig 6 দ্যাখো। এখানে $\mathbb{Z}_4$-এর identity হল 0. দ্যাখো কোন্ কোন্ তীর এই 0-তে গেছে। এই তীরগুলো $\mathbb{Z}_6$-এর যেসব element থেকে বেরিয়েছে, তাদের set-টাকে বলে homomorphism-টার kernel. তার মানে এখানে kernel-টা হল $\{0, 2, 4\}$. এবার সংজ্ঞাটা লিখে নিই।

> DEFINITION: **Kernel**
>
> Let G_1, G_2 be two groups. Let $f : G_1 \to G_2$ be a group homomorphism. Let e_2 be the identity element of G_2. Then the set
>
> $$\{a \in G_1 \ : \ f(a) = e_2\}$$
>
> is called the **kernel** of f, and is denoted by $\ker(f)$.

Exercise 5: যদি homomorphism-টা নিতাম $f : \mathbb{Z}_6 \to \mathbb{Z}_4$ যেখানে $f(x) = x(\text{mod } 3)$, তবে $\ker(f)$ কী হত? ■

Example 6: Show that the mapping $f : (\mathbb{C}', \bullet) \to (\mathbb{R}', \bullet)$ defined by $f(z) = |z|$ for all $z \in \mathbb{C}'$,

where $(\mathbb{C}', \bullet)$ denotes the multiplicative group of nonzero complex numbers and $(\mathbb{R}', \bullet)$ denotes the multiplicative group of nonzero real numbers, is a homomorphism and find $\ker f$.[5] **(2008.4b)**

SOLUTION: প্রথমে দেখাতে হবে যে, f-টা সত্যিই well-defined, অর্থাৎ যে কোনো $z \in \mathbb{C}'$-এর জন্যই $f(z)$-টা $\mathbb{R}'$-এর মধ্যে থাকে--

> We know that if $z \in \mathbb{C}'$ then $f(z) = |z| > 0$. So $f : \mathbb{C}' \to \mathbb{R}'$ is well-defined.

এবার homomorphism দেখাব, মানে--

> Shall show
>
> $\forall w, z \in \mathbb{C}' \quad f(w \bullet z) = f(w) \bullet f(z).$
>
> $\forall w, z$ Take any $w, z \in \mathbb{C}'$.
>
> Then
> $$f(w \bullet z) = |w \bullet z| = |w| \times |z| = f(w) \bullet f(z),$$
> as required.

এবার kernel বার করতে হবে--

> Second part: The identity element of $(\mathbb{R}', \bullet)$ is 1.
>
> So $\ker(f) = \{z \in \mathbb{C}' \ : \ f(z) = 1\} = \{z \in \mathbb{C}' \ : \ |z| = 1\}$. Thus, $\ker(f)$ is the unit circle in the complex plane.

■

নীচের theorem-টা দেখাবে যে, kernel সব সময়েই একটা subgroup হয়।

THEOREM

Let G_1, G_2 be two groups. Let $f : G_1 \to G_2$ be a group homomorphism. Then $\ker(f)$ is a subgroup of G_1.

Proof: এখানেও আমরা subgroup দেখানোর জন্য সেই দুই ধাপের কায়দাটা লাগাব। প্রথম ধাপে nonempty দেখাব--

> Step 1 : We know $f(e_1) = e_2$.
>
> So $e_1 \in \ker(f)$. Hence $\ker(f) \neq \phi$.

এবার দ্বিতীয় ধাপ--

> Step 2 : Shall show
>
> $\forall a, b \in \ker(f) \quad a^{-1}b \in \ker(f).$
>
> $\forall a, b$ Take any $a, b \in \ker(f)$.

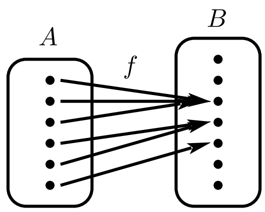


Fig 7

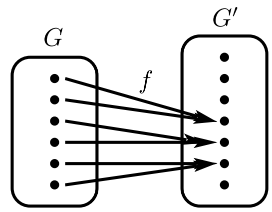


Fig 8

Then

$$\begin{aligned} f(a^{-1}b) &= f(a^{-1})f(b) \quad [\because f \text{ is homomorphism}] \\ &= (f(a))^{-1}f(b) \quad [\because f \text{ is homomorphism}] \\ &= (e_2)^{-1}e_2 = e_2. \end{aligned}$$

So $a^{-1}b \in \ker(f)$, as required.
Thus, $\ker(f)$ is a subgroup of G_1.

[Q.E.D]

একটা homomorphism $f: G_1 \to G_2$ দেওয়া থাকলে সেটা onto বা one-one হবে কিনা সেটা $Im(f)$ এবং $\ker(f)$ দেখে বলে দেওয়া যায়। এর মধ্যে onto-র কায়দাটা তো খুবই সহজ, যদি $Im(f) = G'$ হয় তবেই onto, নইলে নয়। বস্তুতঃ এই কথাটা যে কোনো function-এর বেলাতেই খাটে, তার জন্য f-এর homomorphism হবার কোনো দরকার পড়ে না। কিন্তু one-one-এর ব্যাপারটা একটু জটিল। সেটা একটা ছবি দিয়ে বোঝা যাক। Fig 7-এ একটা function দেখিয়েছি $f: A \to B$. দেখতেই পাচ্ছ যে এটা মোটেই one-one নয়। আমরা f-কে বলি many-to-one, অর্থাৎ একাধিক তীর চিহ্ন একই বিন্দুতে এসে মিলতে পারে। ছবিতে যেমন একটা বিন্দুতে তিনটে এবং আরেকটা বিন্দুতে দুটো তীর চিহ্ন মিশেছে। এ তো গেল এমনি function-এর কথা। একটা homomorphism-ও many-to-one হতে পারে, কিন্তু সেক্ষেত্রে একটা বিশেষ প্যাটার্ণ থাকতে বাধ্য। সেইটা Fig 8-এ দেখিয়েছি। লক্ষ কর যে, এখানে G_2-র কোনো কোনো element-এ কোনো তীর চিহ্নই আসে নি, কিন্তু যেগুলোতে এসেছে সেগুলোতে ঠিক সমান সংখ্যক তীর চিহ্ন এসে মিশেছে, কোনোটায় কম কোনোটায় বেশী এমন নয়। এই প্যাটার্ণটা থাকায় একটা সুবিধা হল, ভাতের হাঁড়িতে যেমন একটা ভাত টিপেই বলে দেওয়া যায়, সবগুলো ভাতের দানা সিদ্ধ হয়েছে কিনা, তেমনি এখানেও কোনো একটা element-এ যদি ঠিক k-খানা তীর চিহ্ন এসে পৌঁছয়, তবে অমনি বলা যায় যে $Im(f)$-এর বাকি প্রত্যেকটা element-এর বেলাতেও ঠিক k-খানাই তীর চিহ্ন আসবে। এই ব্যাপারটা খুব কাজে দেয় one-one পরীক্ষা করার সময়ে। যদি দ্যাখো যে অন্ততঃ একটা element-এও ঠিক একটাই তীর এসে পৌঁছেছে, অমনি জোর দিয়ে বলতে পারবে যে homomorphism-টা one-one হবে। সেই কারণে লোকে সাধারণতঃ one-one পরীক্ষা করার জন্য খালি e_2-এর দিকে (মানে G_2-র identity-র দিকে) তাকায়, দ্যাখে যে সেখানে কতগুলো তীর পৌঁছেছে, মানে কতগুলো $g \in G_1$ আছে যাতে $f(g) = e_2$ হয়। কিন্তু এই সব g নিয়েই তো $\ker(f)$ তৈরী। তাই ব্যাপারটা দাঁড়ায় এইরকম--

> f-টা one-one কিনা বোঝার জন্য খালি $\ker(f)$ দেখলেই চলে, যদি $\ker(f)$-এর সাইজ হয় 1, মানে $\ker(f) = \{e\}$ হয়, তবে (এবং কেবলমাত্র তবেই) f হবে one-one.

এই কথাটা এতই গুরুত্বপূর্ণ যে একে একটা theorem বলা চলে। প্রমাণটা রয়েছে নীচের সমাধানে।

Example 7: Let $\phi: G \to G'$ be a homomorphism of groups. Prove that ϕ is one-to-one if and only if $\ker\phi = \{e_G\}$, where e_G represents the identity element of G. **(2006.3b(part 2))**

SOLUTION:

<u>Step 1:</u> Shall show ϕ one-one $\implies \ker\phi = \{e_G\}$.
$\because f$ is a group homomorphism,
$\therefore \phi(e_G) = e_{G'}$.
$\therefore e_G \in \ker\phi$.
If $g \in \ker\phi$ then $\phi(g) = e_{G'} = \phi(e_G)$.
$\because \phi$ is one-one, $\therefore g = e_G$.
Hence $\ker\phi = \{e_G\}$, as required.

এবার উল্টোদিকটা--

<u>Step 2:</u> Shall show $\ker\phi = \{e_G\} \implies \phi$ one-one, ie,
$\forall g_1, g_2 \in G \quad \big(f(g_1) = f(g_2) \implies g_1 = g_2\big)$.
$\forall g_1, g_2$
Take any $g_1, g_2 \in G$ with $\phi(g_1) = \phi(g_2)$.
Then $\phi(g_1)(\phi(g_2))^{-1} = e_{G'}$.
$\therefore \phi(g_1)\phi(g_2^{-1}) = \phi(g_1 g_2^{-1}) = e_{G'}$, since ϕ is a homomorphism.
$\therefore g_1 g_2^{-1} \in \ker\phi$.
But $\ker\phi = \{e_G\}$.
$\therefore g_1 g_2^{-1} = e_G$,
or, multiplying by g_2 from right, we have $g_1 = g_2$, as required.

■

যা যা শিখলাম, এবার তার একটা প্রয়োগ দেখি।

Example 8: G is a multiplicative commutative group of order 8. Prove that $\Phi : G \to G$ defined by $\Phi(x) = x^3$, $x \in G$ is an isomorphism.[4] **(2012.3b)**

SOLUTION: এতক্ষণ আমরা isomorphism করছিলাম G_1 আর G_2-র মধ্যে। G_1, G_2 যে আলাদা হবেই এমন কিন্তু কোনো কথা নেই। এখানে যেমন দুটোকেই G নেওয়া হয়েছে।

$\because G$ is closed under multiplication,
$\therefore \Phi : G \to G$ is well-defined.

অর্থাৎ কোনো $x \in G$-কে cube করলে আমরা ফের G-এরই একটা element পাব।

$\Phi(xy) = (xy)^3 = xyxyxy = x^3y^3 = \Phi(x)\Phi(y)$.
So Φ is a homomorphism.

এবার one-one দেখাব। তার জন্য দেখাব যে $\ker(\Phi) = \{e\}$, যেখানে e হল G-র identity.

> Let e be the identity of G.
> Then $\Phi(x) = e$ means $x^3 = e$. So $o(x)|3$. But $3 \not| 8$.
> $\therefore o(x) \neq 3$.
> $\therefore o(x) = 1$.
> $\therefore x = e$.
> So Φ is one-one.
> Since G is finite, hence this means Φ is also onto.
> Hence Φ is an isomorphism, as required.

■

DAY 2
নানারকম group

আয় তোর মুণ্ডুটা দেখি, আয় দেখি 'ফুটোস্কোপ' দিয়ে
দেখি কত ভেজালের মেকি, আছে তোর মগজের ঘিয়ে।
-- সুকুমার রায়

পৃথিবীতে মোট কতগুলো group আছে? সংক্ষেপে বলতে গেলে--অসংখ্য। কিন্তু আমরা এখন isomorphism-এর কথা শিখে গিয়েছি, তাই জানি যে এরা আসলে সকলেই একেবারে আলাদা আলাদা group নয়, অনেক ছদ্মবেশী কুমীরছানা মিশে আছে ভেজালের মত। সুতরাং ভেজাল বাদ দিলে সত্যিকারের আলাদা আলাদা group-এর সংখ্যা অপেক্ষাকৃত কম। কিন্তু isomorphic group-দের আলাদা করে না গুণলেও মোট group আছে infinite-সংখ্যক। এদের অনেকের সঙ্গেই আমাদের পরিচয় হয়েছে। এদের মধ্যে কোথাও কোনো ভেজাল লুকিয়ে আছে কিনা দেখা যাক। প্রথমে আলোচনা করি কিছু infinite group-এর কথা--

- $(\mathbb{Z}, +)$: যাবতীয় integer-দের নিয়ে তৈরী group.
- $(\mathbb{Q}, +)$: এই group-টা তৈরী হয়েছে সব rational number-দের নিয়ে।
- $(\mathbb{R}, +)$: এই group-টা আরও বড়, এর সদস্য সব real number.

Example 9: প্রমাণ কর যে $(\mathbb{Q}, +)$ এবং $(\mathbb{Z}, +)$ পরস্পরের সঙ্গে isomorphic নয়।

SOLUTION: এখানে একটু কৌশল করতে হবে। দুটো group-এর মধ্যে কিছু পার্থক্য বার করব। একটা পার্থক্য হল--$\mathbb{Q}$-এর যে কোনো element-কে তুমি যতগুলো খুশী সমান ভাগে ভেঙে ফেলতে পারো যেমন যে কোনো $r \in \mathbb{Q}$ নিলে সেটাকে সমান n ভাগে ভেঙে ফেললে পাই $\frac{r}{n}$ যেটা আবার $\mathbb{Q}$-তেই আছে। এই গুণটা কিন্তু $\mathbb{Z}$-এর নেই। যেমন $1 \in \mathbb{Z}$, কিন্তু ওকে আর ভাঙলে ভগ্নাংশ হয়ে $\mathbb{Z}$-এর বাইরে চলে যাবে। এই পার্থক্যটাকে কীভাবে কাজে লাগাব দ্যাখো--

> Let, if possible, $f : \mathbb{Q} \to \mathbb{Z}$ be a group isomorphism.
> $\because 1 \in \mathbb{Z}, \therefore \exists r \in \mathbb{Q} \quad f(r) = 1$.
> Now $\frac{r}{2} \in \mathbb{Q}$ and $\frac{r}{2} + \frac{r}{2} = r$.
> So applying f to both sides,
>
> $$f\left(\frac{r}{2}\right) + f\left(\frac{r}{2}\right) = f(r) = 1,$$

Thus, $f\left(\frac{r}{2}\right) = \frac{1}{2}\left(\Rightarrow\Leftarrow \because \frac{1}{2} \notin \mathbb{Z}\right)$.

■

Exercise 6: কী করে খুব সহজে দেখাবে যে $(\mathbb{Q}, +)$ এবং $(\mathbb{R}, +)$ পরস্পরের সঙ্গে isomorphic নয়? একই কায়দায় এটাও দেখাতে পারবে যে $(\mathbb{R}, +)$ এবং $(\mathbb{Z}, +)$ পরস্পরের সঙ্গে isomorphic হতে পারে না। ■

আমরা আরেকটা infinite group-এর কথা জানি--$(\mathbb{C}, +)$. এটা যে $(\mathbb{Z}, +)$ বা $(\mathbb{Q}, +)$-এর সঙ্গে isomorphic নয়, সে বিষয়ে আশা করি তোমার সন্দেহ নেই (কারণ cardinality আলাদা)।
আচ্ছা, $(\mathbb{C}, +)$ এবং $(\mathbb{R}, +)$ কি isomorphic? এর উত্তর কিন্তু মোটেই সহজ নয়! বস্তুতঃ এই বইয়ে যা যা শিখেছি বা শিখব, তার ভিত্তিতে এই প্রশ্নটার উত্তর দেওয়া অসম্ভব! তবে উত্তরটার ভিতর একটা মজার ব্যাপার আছে, সেটা বলি। হ্যাঁ, এরা isomorphic, কিন্তু মজাটা হল এই যে, তুমি হাজার চেষ্টা করলেও একটাও isomorphism-এর ফর্মুলা লিখে ফেলতে পারবে না!!! হাতে অফুরন্ত সময় থাকলে চেষ্টা করে দেখতে পারো!
এতক্ষণ যে সব group-এর কথা বললাম তারা সবাই হল additive group, অর্থাৎ group operation-টা হল সাধারণ যোগ। সাধারণ গুণ দিয়েও কিছু infinite group বানানো যায়, খালি তাতে একটা মুস্কিল। যোগের বেলায় উল্টোটা ছিল বিয়োগ, যেকোনো সংখ্যা থেকেই যেকোনো সংখ্যাকে নিশ্চিন্তে বিয়োগ করা যেত। কিন্তু গুণের উল্টো হচ্ছে ভাগ, এদিকে শূন্য দিয়ে আবার কাউকে ভাগ করা যায় না। তাই গুণ দিয়ে group বানানোর সময়ে শূন্যটাকে বাদ দিতে হবে। এইভাবে তিনটে multiplicative group পাব যাদের সাইজ infinite. এরা হল

$$(\mathbb{Q} \setminus \{0\}, \times), (\mathbb{R} \setminus \{0\}, \times) \text{ এবং } (\mathbb{C} \setminus \{0\}, \times)$$

লক্ষ কর যে, $\mathbb{Z}$ থেকে কোনো multiplicative group বানানো যায়নি, কারণ integer-কে integer দিয়ে ভাগ করলে integer নাও পাওয়া যেতে পারে, যেমন $2/3$ মোটেই পূর্ণসংখ্যা নয়।

Exercise 7: দেখাও যে $(\mathbb{C} \setminus \{0\}, \times)$ এবং $(\mathbb{R} \setminus \{0\}, \times)$ পরস্পরের সঙ্গে isomorphic নয়। ভয় নেই এটা সহজে প্রমাণ করা যায়। ■

এবার finite সাইজের কিছু group-এর পরিচয় নেওয়া যাক। নীচের কয়টা কথা এই প্রসঙ্গে অত্যন্ত গুরুত্বপূর্ণ--

1. যেকোনো সাইজ n-এরই অন্ততঃ একটা group হয়, কারণ হাতের পাঁচ $\mathbb{Z}_n$ তো আছেই।

2. যদি n কোনো কিছুর factorial হয়, যেমন $n = 24 (= 4!)$ হলে n সাইজের একটা symmetric group পাওয়া যাবে, যাকে আমরা লিখি S_n. যেমন 24 সাইজের একটা group হল S_4.

3. যদি n একটা prime number হয়, তবে n সাইজের খালি একটাই group সম্ভব (মানে up to isomorphism, যদি একই prime সাইজের দুটো group দ্যাখো, তৎক্ষণাৎ জানবে যে ওরা একই কুমীরছানার দুই ছদ্মবেশ!) এই একমাত্র group-টা হল সেই সবেধন নীলমণি $\mathbb{Z}_n$. সুতরাং দাঁড়ালো এই যে, 1 সাইজের বা prime সাইজের খালি একটা করেই group আছে।

এই শেষের জিনিসটা আমরা এখনও প্রমাণ করি নি, প্রমাণটা একটু পরেই আসছে, কিন্তু আগে এদের সাহায্যে পরীক্ষা করে দেখব কোন সাইজের কটা group আছে। আলোচনাটাকে সংক্ষিপ্ত রাখার জন্য আমরা খালি 1 থেকে 7 সাইজের কতগুলো করে group আছে সেটা বার করেই সন্তুষ্ট থাকব।

1. একটা group-এ আর কিছু না থাক, identity-টা অন্ততঃ থাকবেই, ওটুকু ওরা মায়ের পেট থেকে পড়ার সময়ে সঙ্গে নিয়েই জন্মায়। তাই size zero group বলে কিছু হয় না। সবচেয়ে যেটি ছোটো, সেটির সাইজ 1. মনে রেখো যে 1 সাইজের group একটাই-- আমরা যদি group operation-টাকে $+$ হিসেবে লিখি, তবে এই group-টাকে লেখা যায় $(\{0\}, +)$ বা $\mathbb{Z}_1$.

2. যেহেতু 2 হল prime, তাই 2 সাইজের group-ও আছে একটাই-- $\mathbb{Z}_2$.
3. একইভাবে 3 সাইজের group-ও একখানাই আছে, $\mathbb{Z}_3$.
4. 4 সাইজের group আছে ঠিক দুটো--একজন তো $\mathbb{Z}_4$. অন্যজন হল Klein's 4-group বা K_4. সুতরাং যদি কখনও 4 সাইজের কোনো group পাও, তৎক্ষণাৎ জানবে যে সেটা হয় $\mathbb{Z}_4$-এর সঙ্গে isomorphic, আর নয়তো K_4-এর সঙ্গে isomorphic.
5. 5 হল একটা prime সংখ্যা। অতএব 5 সাইজের একটাই group সম্ভব, সেটা হল $\mathbb{Z}_5$.
6. 6 সাইজের দুটো group-এর খবর আমরা ইতিমধ্যেই পেয়েছি--$\mathbb{Z}_6$ এবং S_3. এরা যে পরস্পরের সঙ্গে isomorphic নয়, তাও জানি (কারণ একজন Abelian, অন্যজন নয়)। নতুন খবর হল এই যে, এরা ছাড়া 6 সাইজের আর কোনো group নেই!
7. 7 সাইজের group বলতে আছে খালি একটাই--$\mathbb{Z}_7$, কারণ 7 হল prime.

আলোচনাটা আমরা 8 বা তার চেয়েও বড় সাইজের group-এর জন্যও চালাতে পারতাম, কিন্তু group-এর সংখ্যা এরপর থেকে ক্রমশঃ বাড়তে থাকে, এবং তাদের হিসেব রাখাও উত্তরোত্তর কঠিন হতে থাকে।
এইবার আমরা যা যা নতুন কথা বলেছি সেগুলো একে একে প্রমাণ করব। এবং তার জন্য আমাদের কাজে লাগবে cyclic group.

2.1 Cyclic groups

আমরা জানি যে, দুটো group যদি isomorphic হয়, তবে তারা আসলে একই group, খালি হয়তো লেখার কায়দাটা আলাদা। সুতরাং G_1 যদি G_2-এর সঙ্গে isomorphic হয়, তবে G_2-ও G_1-এর সঙ্গে isomorphic হতে বাধ্য। আবার ওদের মধ্যে একজন যদি cyclic হয়, তবে অন্যজনও তাই হবে। এটাই ফলাও করে দেখাতে বলেছে নীচের অংকটায়।

Example 10: Let $f : (G, \circ) \to (G', \star)$ be an isomorphism of groups. Prove that G' is cyclic if and only if G is cyclic.[5] **(2009.4b)**

SOLUTION:

<u>Step 1:</u> Shall show G cyclic $\implies G'$ cyclic.

Given, G is cyclic.

Let $c \in G$ be a generator.

অর্থাৎ G-এর প্রতিটা element-কেই c-এর power হিসেবে লেখা যায়।

Shall show that G' is a cyclic group generated by $f(c)$, ie,

$\forall g' \in G' \quad \exists n \in \mathbb{Z} \quad g' = (f(c))^n$.

$\forall g'$ Take any $g' \in G'$.

$\because f : G \to G'$ is onto, $\therefore \exists g \in G \quad f(g) = g'$.

$\because G$ is a generated by c, $\therefore \exists n \in \mathbb{Z} \quad g = c^n$.

$\exists n$ Choose this $n \in \mathbb{Z}$.

$\because f$ is a homomorphism,

> $\therefore g' = f(g) = f(c^n) = (f(c))^n$, as required.

এবার উল্টোদিকটা। কিন্তু এখানে নতুন করে আর কিছু করার নেই, আগের যুক্তিতেই কাজ চলবে--

> Step 2: Since G' is isomorphic to G, hence G is isomorphic to G'. So interchanging the roles of G and G' above, the converse is also proved.

■

লক্ষ কর যে, এখানে step 1-এ আমরা খালি onto ব্যবহার করেছি। সুতরাং isomorphism-এর বদলে epimorphism (অর্থাৎ, একটা homomorphism, যেটা onto) দিলেও step 1-এর যুক্তিটা কাজ করত। সেটাই চেয়েছে নীচের অংকটায়।

Example 11: Let $(G, \circ)$ and $(G', \star)$ be two groups and $\phi : G \to G'$ be an epimorphism. If $(G, \circ)$ is cyclic, prove that $(G', \star)$ is also cyclic. Is it true that $(G, \circ)$ is cyclic when $(G', \star)$ is cyclic? Justify your answer.[2+3] **(2013.3b)**

SOLUTION: প্রথম অংশটা আগের অংকের সমাধানের step 1-এই আছে। এবার দ্বিতীয় অংশ--

> Second part: No, it is possible to have G non-cyclic even when G' is cyclic.
>
> Counterexample: Let G be Klein's 4-group and G' be the trivial group $\{e\}$. Then the map $f : G \to G'$ defined as
>
> $$\forall g \in G \quad f(g) = e$$
>
> is an epimorphism. Here G' is a cyclic group (generated by e). But G is not cyclic, because no element of G has order 4.

■

দুটো group যদি isomorphic হয়, তবে তাদের যাবতীয় group-ঘটিত বৈশিষ্ট্য এক হতে বাধ্য। বিপরীতপক্ষে যদি দুটো group-এর মধ্যে বিভিন্ন বৈশিষ্ট্য একই রকম দ্যাখো, তবে সন্দেহ করবে ওরা হয়তো আসলে isomorphic. কিন্তু বৈশিষ্ট্যগুলোর মধ্যে কতটা মিল থাকলে এ কথাটা জোর দিয়ে বলা যাবে? একটা উদাহরণ হল-- যদি দুটোই cyclic হয় এবং দুজনেরই সাইজ একই হয়, তবে isomorphic হবেই। এটাই নীচের অংকটার বক্তব্য।

Example 12: Show that two finite cyclic groups of the same order are isomorphic.[4] **(2011.3b,2007.4b)**

SOLUTION:

> Let G, H be two finite cyclic groups of order n.

Cyclic মানে একটা element দিয়ে generated, অর্থাৎ group-এর সব element-কেই সেই element-টার power হিসেবে লেখা যাবে। এই রকম বিশেষ element-কে বলে একটা generator.

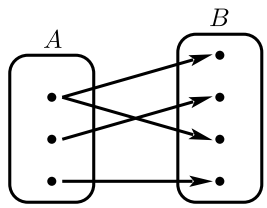


Fig 9

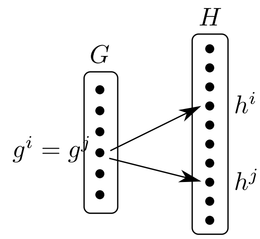


Fig 10

> Let g be a generator of G, and h be a generator of H.
> Then
> $$G = \{g^0, ..., g^{n-1}\},$$
> $$H = \{h^0, ..., h^{n-1}\}.$$

মনে রেখো যে g^0 মানে হল G-র identity element. এখানে আমরা g^{n-1}-এ এসে থেমে গেলাম কেন? কারণ g-এর order হল n. তাই g^n ফের identity element হয়ে যাবে। তারপর $g^{n+1} = g^n g^1 = g^1$ হবে, এইভাবে $g^0, ..., g^{n-1}$ বার বার ফিরে ফিরে আসবে। একই রকম কথা h-এর ক্ষেত্রেও খাটবে।

> Notice that
> $$\forall i, j \in \mathbb{Z} \quad (g^i = g^j \iff i \equiv j (\text{mod } n) \iff h^i = h^j).$$

G আর H-এর দিকে তাকালেই বুঝতে পারছ যে, ওদের কাঠামো আসলে একই। খালি g-এর জায়গায় h লেখা হয়েছে, এই যা তফাৎ। সুতরাং আমরা isomorphism-টা নেব এইভাবে $f(g^i) = h^i$. কিন্তু প্রথমে দেখতে হবে এটা আদৌ well-defined কিনা। এই "well-defined" ব্যাপারটা একটু বোঝা যাক। Fig 9-এ যে তীর চিহ্নগুলো দেখানো হয়েছে, তারা মিলে কিন্তু একটা function হয় না। এটাকেই আমরা একটু জোর দিয়ে বলি যে, ওই তীর চিহ্নগুলো মিলে কোনো well-defined function হয় না। এখানে আমাদের function-টার well-defined হবার পথে একটাই সমস্যা আসতে পারে--সেটা হল যদি এমন i, j থাকে যাতে $g^i = g^j$ হয় কিন্তু $h^i \neq h^j$ হয়ে যায়। সেক্ষেত্রে G-এর একই element g^i (বা g^j) থেকে দুটো তীর চিহ্ন বেরোবে Fig 10-এর মত। কিন্তু সে সমস্যাটা আসলে হবে না, কারণ এক্ষুণি বলে নিয়েছি যে $g^i = g^j \iff h^i = h^j$.

> So the function $f : G \to H$ defined as $f(g^i) = h^i$ is well-defined.

এইবার ধাপে ধাপে এগোব। প্রথমে দেখাব যে f একটা group homomorphism.

> Shall show
> $\forall a, b \in G \quad f(ab) = f(a)f(b).$
> $\forall a, b$ Take any $a, b \in G$.
> Then $a = g^i$ and $b = g^j$ for some $i, j \in \{0, ..., n-1\}$.
> Let $r \in \{0, ..., n-1\}$ be such that $i + j \equiv r (\text{mod } n)$.

অর্থাৎ, $i + j$-কে n দিয়ে ভাগ করে ভাগশেষটাকে r বললাম।

> Then
> $$f(ab) = f(g^{i+j}) = f(g^r) = h^r = h^{i+j} = h^i h^j = f(a)f(b),$$
> as required. Hence f is a group homomorphism.

এবার onto দেখাব--

> Take any $b \in H$.
> Then $b = h^i$ for some $i \in \{0, ..., n-1\}$.
> Hence $f(g^i) = h^i = b$.
> So onto.

সবশেষে one-one দেখাব। সেখানে এটা ব্যবহার করব যে, G এবং H দুজনেই finite, এবং একই সাইজের। সুতরাং ওদের মধ্যে কোনো function-এর পক্ষে onto হওয়া আর one-one হওয়া সমার্থক।

> Since $|G| = |H| < \infty$, $\therefore$ any onto onto function from G to H must also be one-one.
> Hence f must be one-one, and so G, H are isomorphic, as required.

■

নীচের অংকটা একইরকম, খালি এখানে যে কোনো cyclic group না বলে $(\mathbb{Z}_n, +)$ বলেছে (এখানে $+$ মানে কিন্তু $\oplus$ বুঝতে হবে)। এটা তোমার করার জন্য রেখে দিলাম।

Exercise 8: Prove that a finite cyclic group of order n is isomorphic to $(\mathbb{Z}_n, +)$.[4] **(2009.3b)**
■

আমরা আগেই শিখেছি যে, prime সাইজের group-রা সব সময়ে cyclic হয়। সুতরাং পেলাম--যদি দুটো group-এর সাইজ একই prime সংখ্যা হয়, তবে ওরা isomorphic না হয়ে যায় না। ঠিক এই কথাটাই আমরা একটু আগে ব্যবহার করেছিলাম--যে কোনো prime p সাইজের ঠিক একটা করেই group সম্ভব, এবং সেটা হল $\mathbb{Z}_p$.
একই যুক্তি অবশ্য infinite group-এর ক্ষেত্রেও খাটে, cyclic হলেই হল। তা নিয়েই নীচের অংক দুটো--

Example 13: Prove that two infinite cyclic groups are isomorphic to each other.[5] **(2008.3b)**

SOLUTION: Example 12-এর মতই। ■

Example 14: Prove that an infinite cyclic group is isomorphic to the group $(\mathbb{Z}, +)$, ($\mathbb{Z}$ is the set of all integers).[4] **(2006.4b)**
SOLUTION: প্রথমে আগের অংকটা কর। এটা একেবারে একই জিনিস, খালি যে কোনো infinite cyclic group-এর জায়গায় $(\mathbb{Z}, +)$ দিয়েছে। ■

আমরা বলেছিলাম যে, 4 সাইজের ঠিক দুটোই group সম্ভব--$\mathbb{Z}_4$ এবং K_4 Klein's 4-group.এবার সেটা প্রমাণ করা নিয়ে কিছু অংক করি। আমরা আগেই বলেছি যে, ওরা পরস্পরের সঙ্গে isomorphic নয়, কারণ $\mathbb{Z}_4$ হল *cyclic*, কিন্তু K_4

	e	a	b	c
e	e	a	b	c
a	a			
b	b			
c	c			

Fig 11

	e	a	b	c
e	e	a	b	c
a	a	e		
b	b		e	
c	c			e

Fig 12

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Fig 13

মোটেই cyclic নয়। নীচের অংকটা দেখাতে বলেছে যে, অন্য যেকোনো 4 সাইজের group ওদের মধ্যে একজনের সঙ্গে isomorphic হতে বাধ্য।

Exercise 9: দেখাও যে G যদি কোনো 4 সাইজের group হয়, তবে G-টা হয় $\mathbb{Z}_4$ আর নয়তো K_4-এর সঙ্গে isomorphic.

HINT:

মূল ধারণাটা দিচ্ছি, গুছিয়ে লেখার দায়িত্ব তোমার। $o(G) = 4$ বলা আছে। সুতরাং G-এর যে কোনো element-এর order কী কী হতে পারে? উত্তর--$1, 2$ বা 4. এর মধ্যে order 1 তো খালি একজনেরই হবে, সে হল identity. বাকিদের ভাগে রইল 2 আর 4.

যদি একজনেরও order 4 হয়, তবে G-টা cyclic হতে বাধ্য, সুতরাং G সেক্ষেত্রে $\mathbb{Z}_4$-এর সঙ্গে isomorphic.

পড়ে রইল খালি একটাই কেস--যেখানে identity ছাড়া বাকিদের প্রত্যেকের order হল 2. আমরা আগেই শিখেছি যে এক্ষেত্রে G-কে Abelian হতে হবে। সুতরাং যদি $G = \{e, a, b, c\}$ হয় তবে নামতার টেবিলটা পূর্ণ করা সহজ--যেহেতু e দিয়ে গুণ করলে সব element-ই অপরিবর্তিত থাকে, তাই শুরুতে যে Fig 11-র মত হবে তাতে সন্দেহ নেই। আবার বলেছে যেকোনো element-কেই square করলে e হয়ে যায় তাই Fig 12-এর মত হবে। আরো লক্ষ কর যে $ab = c$ হওয়া ছাড়া গত্যন্তর নেই, কারণ $ab = a$ হলে $b = e$ হয়ে যাচ্ছে, $ab = b$ হলে $a = e$ হয়ে যাবে, আর $ab = e$ হলে $a = b$ হয়ে যাবে কারণ $a^2 = e$. একই যুক্তিতে $ba = c, ac = b, ca = b, cb = a$ এবং $bc = a$ হতেও বাধ্য। সুতরাং নামতার টেবিলটা দাঁড়াচ্ছে Fig 13-এর মত। ব্যস্, এটাই তো K_4-এর নামতা! যদি চিনতে না পারো, তবে জলের molecule-এর নামতার সঙ্গে তুলনা করে দেখতে পারো (a, b, c-র বদলে r, s_1, s_2 বসালেই হবে)। ■

এবার একটু প্রসঙ্গে পালটাই । আমরা দেখেছি যে দুটো cyclic group-এর সাইজ সমান হলেই ওরা isomorphic হয়ে যায়। Abelian group-দের বেলাতেও কি কথাটা খাটে? সেইটা নিয়েই এবারের অংক।

Exercise 10: Two finite groups are of same order and are both Abelian. Must they be isomorphic? ■

DAY 3
Normal subgroup (part 1)

ছোটোবেলায় রূপকথার গল্পে অনেক সময়ে এরকম ব্যাপার থাকত--এক বাড়ির তিন ভাইয়ের মধ্যে ছোটো ভাইটা খুব ভালো আর সৎ, কিন্তু বড় দুটো ভাই বেজায় দুষ্টু। তারা বেচারী ছোটো ভাইকে ঠকিয়ে সব সম্পত্তি হাত করে নিয়েছে। ছোটো ভাই একা একা বনের ধারে কুঁড়ে ঘরে থাকে আর কাঠ কেটে সংসার চালায়। এদিকে তো সেই রাজ্যের রাজার মেয়েকে রাক্ষস-টাক্ষস কিছু একটা এসে হরণ করে নিয়ে গেছে। প্রথমে বড় দুটো ভাই রাজকন্যাকে উদ্ধার করতে গিয়ে নাস্তানাবুদ। তারপর ছোটোভাইয়ের পালা। সে তো কিছুই জানে না রাজকন্যা কী করে উদ্ধার করতে হয়। এমন সময়ে কোথা থেকে এক বুড়ি এসে তাকে একটা চিরুণী দিল। সে চিরুণীর আশ্চর্য গুণ--তার গায় ফুঁ দিলেই সেটা একটা আয়না হয়ে যায়। তাতে রাজকন্যা উদ্ধারের কী সুবিধা

হয়, সেটা অবশ্য তখনই বোঝা যায় না। কিন্তু কি আশ্চর্য, গল্পের শেষে দেখা যায় যে, রাক্ষস মারতে ঠিক এমন একটা চিরুণীরই দরকার ছিল (কারণ চিরুণীর গুণ এবং গল্পের প্লট একই লেখকের উর্বরমস্তিষ্কপ্রসূত)।
অংকের জগতেও মাঝে মাঝে এরকম চিরুণীর দেখা মেলে। এদের definition-গুলো দেখতে সহজ, কিন্তু কেন এমন definition দিয়ে সুবিধা হবে, গোড়ায় সেটা কিছুই বোঝা যায় না। পরে অনেক কিছু শেখার পর দেখা যায় হঠাৎ সেটা কাজে লাগছে। এসব ক্ষেত্রে definition-টা কী সেটা বোঝা সেটা বোঝা অতি সহজ, কিন্তু এর দ্বারা আদৌ কী সুবিধা হবে সেটা বুঝতে অনেকটা সময় লাগে। ঐতিহাসিকভাবেও দেখা যায় এই definition-গুলোর জন্ম হয়েছে অনেক পরে। কোনো একটা ব্যাপার হয় তো বিভিন্ন জায়গায় বার বার কাজে লাগছে। এই ঘটনা বহুবার লক্ষ করার পর পণ্ডিতেরা প্রথম তার গুরুত্ব অনুধাবন করেছেন, এবং সেটাকে একটা definition-এর মর্যাদা দিয়েছেন। অংকের বিভিন্ন শাখাতেই এরকম "চিরুণী"-র দেখা মেলে, যেমন

- real analysis-এ compactness,
- linear algebra--তে matrix,
- group theory-তে normal subgroup, যেটা আমরা এবার শিখব।

3.1 কাকে বলে?

আমরা জানি একটা group-এর subgroup বলতে কি বোঝায়। এদের মধ্যে একটা বিশেষ ধরণের subgroup-কে বলে **normal subgroup**. এর ধারণাটা প্রথম যখন এসেছিল তখন এর গুরুত্ব কেউ তেমন বোঝে নি। পরে Evariste Galois (এভারিস্তে গ্যালোয়া) নামের এক গণিতজ্ঞ একটা গুরুত্বপূর্ণ অংকের সমাধান করতে গিয়ে লক্ষ করেন যে এই ধারণাটা খুব কাজে লাগছে। তিনিই normal subgroup নামটা দেন। কোন্ গুরুত্বপূর্ণ সমস্যার সমাধান করতে normal subgroup-এর উপযোগিতা প্রথম বোঝা গিয়েছিল, সেটার বর্ণনা করতে পারলে normal subgroup-এর গুরুত্ব বোঝানোটা সহজ হত। কিন্তু দুঃখের বিষয় সেই গুরুত্বপূর্ণ সমস্যাটা বোঝাতে গেলে আরো অনেক কিছু লাগবে যেগুলো এই বইয়ের পাল্লার বাইরে। তাই আমরা ও পথে না গিয়ে অন্যপথে বোঝানোর চেষ্টা করি।

3.2 তিনরকম সংজ্ঞা

Normal subgroup-এর definition বিভিন্নভাবে লেখা যায়। এরা দেখতে কিছুটা আলাদা হলেও সবাই সমার্থক, এবং সেটা খুবই সহজে প্রমাণ করা যায়। প্রথমে এরকম তিনটে definition দিয়ে নিই। তারপর আলোচনা করব, normal subgroup জিনিসটা নিয়ে আদৌ কেন মাথা ঘামাব।

DEFINITION: **Normal subgroup (defn 1)**

Let G be a group, and H be a subgroup of G. Then H is called a **normal subgroup** of G if
$$\forall g \in G \quad gH = Hg.$$

এই সংজ্ঞাটা দেখতে খুবই commutativity-র মত। বস্তুতঃ এখান থেকেই বোঝা যাচ্ছে যে, G যদি Abelian হয়, তবে যে কোনো H-এর জন্যই এই শর্তটা পালিত হবে। যদি Abelian নাও হয়, তাহলেও ব্যাপারটা এইরকম-- ধরো যা খুশি $h \in H$ নিলাম, তাহলে $gh \in gH$. যেহেতু $gH = Hg$, তাই $gh \in Hg$ হবে, মানে এমন $h' \in H$ পাওয়া যাবে, যাতে $gh = h'g$ হয়। ঠিক যেন g-টা h-কে ভেদ করে ওই পাশে চলে গেল, এবং তার ফলে h-টা বদলে হয়ে গেল h' (যদি Abelian হত, তবে h-টা বদলাত না)। এই "ভেদ করে ওপাশে চলে যাওয়া"-র উপমাটা পরে বারবার কাজে দেবে।

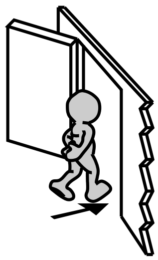


Fig 14

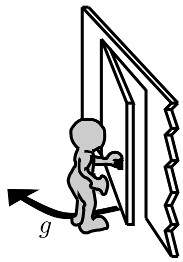


Fig 15

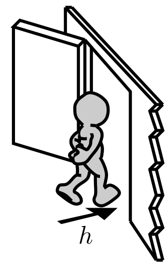


Fig 16

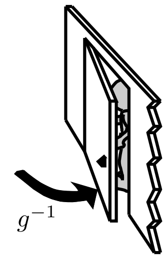


Fig 17

> DEFINITION: **Normal subgroup (defn 2)**
>
> Let G be a group, and H be a subgroup of G. Then H is called a **normal subgroup** of G if
> $$\forall g \in G \quad gHg^{-1} = H.$$

> DEFINITION: **Normal subgroup (defn 3)**
>
> Let G be a group, and H be a subgroup of G. Then H is called a **normal subgroup** of G if
> $$\forall g \in G \quad gHg^{-1} \subseteq H.$$

এই তিনটে সংজ্ঞাই সমার্থক, কিন্তু বোঝাতে সুবিধা হবে শেষেরটা দিয়ে। এতে বলা হয়েছে যে, $h \in H$ এবং $g \in G$ হলে ghg^{-1} থাকবে আবার H-এর মধ্যেই। এই যে আমরা ghg^{-1} নিয়ে কাজ করছি, এর একটা নাম আছে--একে বলে **conjugation** of h by g. এই জিনিসটা আমরা প্রতিদিনের জীবনে হামেশাই ব্যবহার করে থাকি। একটা উদাহরণ দেখলেই চিনতে পারবে। Fig 14 দ্যাখো। একটা ছেলেটা একটা খোলা দরজার সামনে দাঁড়িয়ে আছে। আমরা চাই যেন ও দরজার ওইপাশে গিয়ে দাঁড়ায়, দরজাটা যেমন আছে তেমনই রেখে। সে কাজটা সহজ--সোজা খোলা দরজা দিয়ে হেঁটে চলে গেলেই হল। এবার মনে করো দরজাটা প্রথমে বন্ধ ছিল। এখানেও ছেলেটার প্রতি একই নির্দেশ--দরজার ওইপাশে গিয়ে দাঁড়াতে হবে, দরজা যেন বন্ধই থাকে। এবার ছেলেটা এইভাবে এগোবে--প্রথমে দরজাটা খুলবে (Fig 15), তারপর আগের মতই হেঁটে ওই পাশে যাবে (Fig 16), এবং তারপর দরজাটা ফের বন্ধ করে দেবে (Fig 17)। এখানে দরজা খোলা এবং বন্ধ করা হল পরস্পরের বিপরীত কাজ। যদি খোলাকে g বলি, তবে বন্ধ করাকে g^{-1} বলতে পারি। দরজা দিয়ে হেঁটে যাওয়াকে যদি h বলি তবে বন্ধ দরজার ক্ষেত্রে ছেলেটা যা করল তাকে ghg^{-1} লিখতে পারি। এখানে ওর মূল উদ্দেশ্য ছিল খালি হেঁটে যাওয়া,

Fig 18

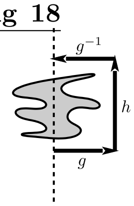
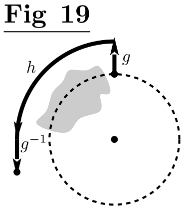


Fig 19



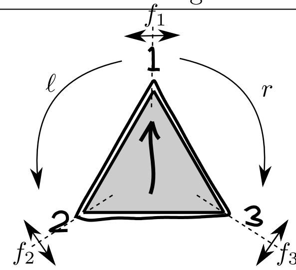


Fig 20

মানে h. কিন্তু দরজা বন্ধ থাকায় তার আগে g করতে হল, আর যেহেতু দরজাটা শেষে আবার বন্ধই রাখতে হবে, তাই আবার পরে g^{-1} করে দিতে হয়েছে। এইভাবে যখনই কোনো কিছুকে বাঁচিয়ে কোনো কাজ করতে হয়, তখনই conjugation-এর প্রয়োজন পড়ে। তোমরা যারা Rubic cube নিয়ে খেলা করেছ, তারা এর প্রয়োজনটা সহজে বুঝবে। Cube-টার খানিকটা সমাধান হয়ে যাবার পরে পরবর্তী ধাপগুলো সাবধানে এগোতে হয়, যাতে হয়ে-যাওয়া অংশগুলো ফের ঘেঁটে না যায়।
এবার normal subgroup-এর তৃতীয় সংজ্ঞাটার দিকে তাকাও। "H হল G-এর একটা normal subgroup" মানে-- $h \in H$ হলে h-এর যে কোনো conjugate-ও H-এ থাকতে বাধ্য। একটা উদাহরণ দিয়ে বোঝা যাক।

Example 15: ধরো তুমি একজন সৈনিক, যুদ্ধক্ষেত্রে তোমাকে নির্দেশ দেওয়া হয়েছে সর্বদা উত্তর-দক্ষিণ লাইন বরাবর

চলতে। এবার ধরো তুমি দেখলে যে, চলার পথে একটা বড় গর্ত (Fig 18), সেটাকে এড়িয়ে যাওয়ার জন্য তুমি একটু নিয়মভঙ্গ করে প্রথমে পশ্চিমে খানিকটা সরে গেলে। তার পর যথারীতি খানিকটা উত্তরে গিয়ে গর্তটা পেরিয়ে আবার যেটুকু পশ্চিমে সরে গেছিলে ততটা পূর্বে ফিরে এলে। ব্যস্‌ তুমি যে নিয়ম ভেঙেছিলে তার কোনো চিহ্নই রইল না। এখানে যেন G হল উত্তর-দক্ষিণ-পূর্ব-পশ্চিম যে কোনো দিকে চলতে পারা। যখন তোমার গতিবিধি খালি উত্তর-দক্ষিণ বরাবর সীমাবদ্ধ করে দেওয়া হল, তখন পেলাম H subgroup-টা। এই subgroup-টার একটা সুবিধা হল যদি তুমি একবার নিয়ম ভাঙো-ও, তবে পরে তার উল্টো কাজটা করে নিলে আবার subgroup-এর ভিতরে ফিরে আসবে। এটাই হল normal subgroup-এর সংজ্ঞা। ■

সব সময়েই যে এমনটা হবে কথা নেই। যেমন ধরো নীচের উদাহরণটা।

Example 16: যদি তোমার প্রতি নির্দেশ থাকত origin-এর থেকে সব সময়ে সমান দূরত্ব বজায় রেখে চলার। তার মানে

নিয়ম মেনে চললে তোমাকে সব সময়ে একটা circular পথে চলতে হবে (Fig 19) এবার ধরো সেই পথের মাঝখানে একটা গর্ত পড়েছে। তাই তুমি প্রথমে খানিকটা উত্তরে সরে গেলে (নিয়ম ভেঙে), তার পর যথারীতি circular পথে গেলে, এবং অবশেষে ওই পরিমাণ দক্ষিণে ফিরে এলে। লক্ষ কর যে তাহলে তুমি তোমার circle থেকে সরে গেলে। মানে, একবার নিয়ম ভঙ্গ করার পরে তার উল্টোটা করে নিলেই সব সময়ে নিয়মভঙ্গের দোষ কেটে যায় না। ■

যেসব subgroup-এর ক্ষেত্রে নিয়মভঙ্গের দোষ কাটাকাটি হয়ে যায়, তাদেরই বলে normal subgroup.
এবার একটা subgroup-এর উদাহরণ দিই, যেটা normal নয়। বুঝতেই পারছ যে এর জন্য একটা non-Abelian group নিয়ে শুরু করতে হবে, কারণ প্রথম সংজ্ঞাটা থেকেই জানি যে, Abelian group-এর বেলায় যেকোনো subgroup-ই normal হবে।
সবচেয়ে ছোটো non-Abelian group হল S_3. এর সাথে পরিচয় আগেই হয়েছে। এটা হল সেই কাগজের ত্রিভুজ ঘুরিয়ে বা উল্টে বসানোর group-টা। এর বিশদ বিবরণ আছে দ্বিতীয় অধ্যায়ে। মনে করার জন্য Fig 20 দেখে নাও।
এর মধ্যে একটা subgroup হল $H = \{e, f_1\}$. আমরা দেখাব যে এটা S_3-র একটা normal subgroup নয়, অর্থাৎ H-এর মধ্যে এমন কোনো element আছে যার অন্ততঃ একটা conjugate গিয়ে পড়ে H-এর বাইরে। এই conjugate-টাকে দ্যাখো--

$$r^{-1} \circ f_1 \circ r.$$

অর্থাৎ প্রথমে টুকরোটাকে একঘর ডানদিকে ঘোরাও, তারপর ফ্রেমের 1 নম্বর প্রান্তটাকে স্থির রেখে উল্টে দাও, তারপর ওল্টানো টুকরোটাকে একঘর বাঁদিকে ঘোরাও। (মনে রেখো, এখানে binary operation-টা হল function composition, তাই

ডানদিক থেকে বাঁদিকে পড়ছি)। এর ফলে মোট যে পরিবর্তনটা হল সেটা কি H-এর মধ্যে আছে? মানে সেটা কি e বা f_1? নিজের হাতে করে দেখলেই বুঝবে যে তা নয়।

3.3 তিনটে সংজ্ঞাই সমার্থক

এইবার আমরা দেখাব যে, তিনটে definition-ই সমার্থক। প্রথম আর তৃতীয় definition নিয়ে নীচের অংকটা।

Example 17: Prove that a subgroup $(H, \circ)$ of a group $(G, \circ)$ is normal if and only if for every $a \in G \implies aHa^{-1} \subset H$.[4] **(2012.3a)**

SOLUTION: এই অংকে $\subset$ চিহ্নটা $\subseteq$ অর্থেই ব্যবহৃত হচ্ছে।

> Want to show that the following two statements are equivalent:
> (1) H is normal in G, ie, $\forall g \in G \quad gH = Hg$.
> (2) $\forall a \in G \quad aHa^{-1} \subset H$.

লক্ষ কর, এখানে আমরা normal-এর প্রথম সংজ্ঞাটা নিয়েছি। যেহেতু তৃতীয় সংজ্ঞাটা প্রমাণ করতে বলেছে, তাই সেটা নিয়েই তো আর শুরু করা যায় না। আর দ্বিতীয় সংজ্ঞাটা তো তৃতীয়টার খুবই কাছাকাছি, তাই সেটাও নিই নি।

> (1) $\implies$ (2):
> Take any $a \in G$.
> Take any $x \in aHa^{-1}$. Then $\exists h \in H \quad x = aha^{-1}$.

এবার a-টা h-কে ভেদ করে ডানদিকে চলে যাবে (ফলে h-টা হয়তো বদলে কোনো h' হয়ে যাবে)।

> Now $ah \in aH = Ha$.
> $\therefore \exists h' \in H \quad ah = h'a$.
> $\therefore x = aha^{-1} = h'aa^{-1} = h' \in H$.
> Thus $aHa^{-1} \subseteq H$, as required.

এবার উল্টো দিকটা--

> (2) $\implies$ (1):
> Take any $g \in G$.
> We pick any $x \in gH$.
> Then $\exists h \in H \quad x = gh$.
> Now $xg^{-1} \in gHg^{-1} \subseteq H$.
> Let $h = xg^{-1}$.
> Then $x = hg \in Hg$. Hence $gH \subseteq Hg$.

এবার আমরা একইভাবে দেখাব যে $Hg \subseteq gH$.

> We pick any $y \in Hg$.
> Then $\exists h' \in H \quad y = h'g$.
> Now $g^{-1}y \in g^{-1}Hg \subseteq H$.
> Let $h'' = g^{-1}y$.
> Then $y = gh'' \in gH$. Hence $Hg \subseteq gH$.
> So $gH = Hg$, as required.

■

সুতরাং প্রথম আর তৃতীয় সংজ্ঞাদুটো যে সমার্থক, সেটা দেখা গেল। দ্বিতীয় আর তৃতীয় সংজ্ঞাদুটো যে একই জিনিস সেটা দেখা আরও সহজ। দ্বিতীয় সংজ্ঞা অনুযায়ী যদি H একটা normal subgroup হয়, তবে যে তৃতীয় সংজ্ঞা অনুযায়ীও তাই হবে, তাতে নিশ্চয়ই সন্দেহ নেই, কারণ $gHg^{-1} = H$ হলে অবশ্যই $gHg^{-1} \subseteq H$-ও বটে। বাকি থাকে খালি তৃতীয় সংজ্ঞা থেকে দ্বিতীয় সংজ্ঞাতে পৌঁছনো।

Exercise 11: দেখাও যে H যদি তৃতীয় সংজ্ঞা অনুসারে G-এর একটা normal subgroup হয়, মানে

$$\forall g \in G \quad gHg^{-1} \subseteq H \tag{*}$$

হয়, তবে দ্বিতীয় সংজ্ঞা অনুসারেও হবে, মানে

$$\forall g \in G \quad gHg^{-1} = H$$

হবে।

HINT:
এই অংকটা তুমিই করবে, খালি একটু ধরিয়ে দিই। প্রথমে যা খুশী একটা $g \in G$ নেবে। দেখাতে হবে $gHg^{-1} = H$. এর মধ্যে $gHg^{-1} \subseteq H$ তো দেওয়াই আছে। সুতরাং $H \subseteq gHg^{-1}$ দেখালেই হবে। যে কোনো একটা $h \in H$ নাও। লক্ষ কর যে (*)-এ g-এর জায়গায় g^{-1} বসালে $g^{-1}Hg \subseteq H$ হচ্ছে। সুতরাং $g^{-1}hg \in g^{-1}Hg \subseteq H$. এটার একটা নাম দিই--

$$h' = g^{-1}hg \in H.$$

এবার দ্যাখো তো h-কে h' আর g দিয়ে লিখতে পারো কিনা। সেখান থেকে কি $h \in gHg^{-1}$ পাওয়া যাচ্ছে? ■

3.4 পাঁচমিশালী অংক

Example 18: Let H be a subgroup of a group G such that $[G : H] = 2$. Prove that H is a normal subgroup of G. Is the converse true? Justify your answer.[4] **(2006.3a)**

SOLUTION: আশা করি ভুলে যাওনি যে $[G : H]$ মানে G-এর মধ্যে H-এর কতগুলো coset আছে। এর পোশাকী নাম হল **index** of H in G.

> First part: Given, $[G : H] = 2$, ie, H has only two distinct (left) cosets in H.

এখানে left কথাটাকে ব্র্যাকেটের মধ্যে রেখেছি, কারণ left coset আর right coset-দের সংখ্যা সব সময়ে সমান হয়। তাই আমরা right coset-দের নিয়েও কাজ করে পারতাম।

Shall show H is normal in G.

এখানে আমরা প্রথম সংজ্ঞাটা ব্যবহার করব। এর পিছনে কোনো বিশেষ কারণ নেই, অন্য দুটো ব্যবহার করলেও চলত।

Enough to show

$\forall g \in G \quad gH \subseteq Hg.$

$\forall g$ Take any $g \in G$.

Case 1: $g \in H$:

$\because H$ is a subgroup, hence closed under the group operation.

$\because gH \subseteq H$. Since distinct (left) cosets are disjoint,

$\therefore gH = H$.

Similarly, $Hg = H$.

Thus $gH = Hg$.

Case 2: $g \notin H$:

$\because g \notin H$, $\therefore gH \neq H$.

Since H has only two distinct (left) cosets in G,

$$gH = G \setminus H.$$

Similarly, $Hg = G \setminus H$.

Thus, again $gH = Hg$.

Hence H is normal in G, as required.

■

Example 19: Let H, K be normal subgroups of a group G. Prove that KH and HK are both normal in G, where $KH = \{kh \;:\; k \in K,\; h \in H\}$ and $HK = \{hk \;:\; h \in H,\; k \in K\}$.[4] **(2012.4b)**

SOLUTION: আমরা আবার প্রথম সংজ্ঞাটা লাগাব--

Shall show

$\forall g \in G \quad gHK = HKg.$

এটা কেন হবে সেটা বোঝা খুবই সহজ। H-টা যেহেতু normal, তাই g-টা H-এর ডানদিকে চলে যেতে পারবে, $gHK = HgK$. আবার K-টাও তো normal, সুতরাং g-টা K-রও ডানদিকে চলে যাবে, $HgK = HKg$. তবে এই জিনিসটা একেবারে সরাসরি লিখে দেওয়া যাবে না, কারণ এখানে আমরা এক ধরণের associativity-র মত জিনিস ব্যবহার করেছি--$gHK = (gH)K = (Hg)K = H(gK) = H(Kg)$. যেহেতু এখানে binary operation-টা হচ্ছে একটা element-এর সঙ্গে একটা subgroup-এর, তাই এটা ঠিক সাধারণ associativity নয়। সেই জন্যই যেটুকু লিখতে হবে।

$\forall g$ Take any $g \in G$.

দুটো set-কে সমান দেখাতে হবে, gHK আর HKg. সুতরাং--

Take any $x \in gHK$.
Then $x = ghk$ for some $h \in H$ and some $k \in K$.

এবার g-টা h-কে ভেদ করে চলে যাবে, ফলে h-টা হয়তো বদলে কোনো h' হয়ে যাবে--

Now $gh \in gH = Hg$, since H is normal in G.
So $gh = h'g$ for some $h' \in H$.
So $x = ghk = h'gk$.

এবার আবার g-টা k-কে ভেদ করে ওই পাশে চলে যাবে--

Again, $gk \in gK = Kg$, since K is normal in G.
So $gk = k'g$ for some $k' \in K$.
So $x = h'gk = h'k'g \in HKg$.
Hence $gHK \subseteq HKg$.

এবার দেখানো উচিত $HKg \subseteq gHK$. কিন্তু সেটা তো ঠিক একই যুক্তিতে হবে। তাই--

By similar arguement, $HKg \subseteq gHK$.
Hence $HKg = gHK$.
Thus HK is normal in G, as required.

■

Example 20: Let M and N be two normal subgroups of a group G such that $M \cap N = \{e\}$, where e is the identity of G. Prove that $mn = nm \quad \forall m \in M$ and $\forall n \in N$.[3] **(2009.4a,2007.4a)**
SOLUTION:

To show
◎ $\forall m \in M \quad \forall n \in N \quad mn = nm.$

আমাদের কায়দাটা হবে এইরকম। আমরা দেখাব $mn(nm)^{-1}$-টা M-এও আছে, আবার N-এও আছে। যেহেতু $M \cap N = \{e\}$, তাই এ থেকেই পেয়ে যাব $mn(nm)^{-1} = e$, মানে $mn = nm$.

$\forall m, n$ Take any $m \in M$ and any $n \in N$.

Then

$$\begin{aligned} mn(nm)^{-1} &= mnm^{-1}n^{-1} \\ &= n'mm^{-1}n^{-1} \quad [\text{ for some } n' \in N, \text{ as } N \text{ is normal.}] \end{aligned}$$

সেই ভেদ করে যাওয়ার গল্প। m-টা n-কে ভেদ করে গেল।

$$= n'n^{-1} \in N,$$

since N is closed under multiplication.

এবার একই কাজ করব M-কে নিয়ে--

Again,

$$\begin{aligned} mn(nm)^{-1} &= mnm^{-1}n^{-1} \\ &= mnn^{-1}m' \quad [\text{ for some } m' \in M, \text{ as } M \text{ is normal.}] \end{aligned}$$

এখানেn^{-1}-টা $m^{-1} \in M$-কে ভেদ করে গেল।

$$= mm' \in M,$$

since M is closed under multiplication.

এবার উপসংহার--

Thus $mn(nm)^{-1} \in M \cap N$.
But $M \cap N = \{e\}$,
$\therefore mn(nm)^{-1} = e$,
or $mn = nm$, as required.

■

Example 21: $(G, \circ)$ and $(G', \star)$ are two groups. $f : G \to G'$ is an onto homomorphism. Prove that if H is a normal subgroup of G then $f(H)$ is also a normal subgroup of $(G', \star)$.[4] **(2010.3b)**

SOLUTION: দুই ধাপে করব--প্রথমে দেখাব subgroup, তারপর দেখাব যে সেটা normal.

Step 1: To show $f(H)$ is a subgroup of G'.

Subgroup দেখানোর কায়দা তো জানোই--

Clearly $e \in H$, and so $f(e) \in f(H)$.
$\therefore f(H) \neq \phi$.
Take any $g_1', g_2' \in f(H)$.
Then $g_1' = f(h_1)$ and $g_2' = f(h_2)$ for some $h_1, h_2 \in H$.

Since f is a homomorphism,

$$\therefore g_1^{-1}g_2 = (f(h_1))^{-1}f(h_2) = f(h_1^{-1})f(h_2) = f(h_1^{-1}h_2) \in f(H),$$

Thus $f(H)$ is a subgroup of G'.

এবার normal দেখানোর পালা--

Step 2: To show $f(H)$ is normal in G',

ie,

$$\forall g' \in G' \quad g'f(H)(g')^{-1} \in f(H),$$

ie,

◎ $\forall a \in G' \quad \forall h \in H \quad af(h)a^{-1} \in f(H).$

$\forall a, h$ Take any $a \in G'$ and any $h \in H$.

$\because f : G \to G'$ is onto, $\therefore \exists g \in G \quad f(g) = a.$

$\because f$ is a homomorphism,

$\therefore af(h)a^{-1} = f(g)f(h)(f(g))^{-1} = f(g)f(h)f(g^{-1}) = f(ghg^{-1}).$

Now, $\because H$ is normal in G, $\therefore gHg^{-1} \subseteq H.$

Thus $ghg^{-1} = h'$ for some $h' \in H.$

So $f(ghg^{-1}) = f(h') \in f(H)$, as required.

■

Example 22: Let

$$G = \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \; : \; a, b, c \text{ are real and } ac \neq 0 \right\}$$

be a group under matrix multiplication. Show that

$$N = \left\{ \begin{bmatrix} 1 & c \\ 0 & 1 \end{bmatrix} \; : \; c \text{ is real number} \right\}$$

is a normal subgroup of G.[3] **(2013.4a)**

SOLUTION:

Enough to show that

$$\forall g \in G \quad gNg^{-1} \subseteq N,$$

ie,

◎ $\forall g \in G \quad \forall n \in N \quad gng^{-1} \in N.$

$\forall g, n$ Take any $g \in G$ and any $n \in N$.

Then

$$g = \begin{bmatrix} a & b \\ 0 & c \end{bmatrix},$$

for some $a, b, c \in \mathbb{R}$ with $ac \neq 0$, and

$$n = \begin{bmatrix} 1 & d \\ 0 & 1 \end{bmatrix},$$

for some $d \in \mathbb{R}$.
So

$$\begin{aligned}
gng^{-1} &= \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \begin{bmatrix} 1 & d \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a & b \\ 0 & c \end{bmatrix}^{-1} \\
&= \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \begin{bmatrix} 1 & d \\ 0 & 1 \end{bmatrix} \frac{1}{ac} \begin{bmatrix} c & -b \\ 0 & a \end{bmatrix} \quad [\because ac \neq 0] \\
&= \frac{1}{ac} \begin{bmatrix} a & ad+b \\ 0 & c \end{bmatrix} \begin{bmatrix} c & -b \\ 0 & a \end{bmatrix} \\
&= \frac{1}{ac} \begin{bmatrix} ac & -ab + a(ad+b) \\ 0 & ac \end{bmatrix} \\
&= \begin{bmatrix} 1 & \frac{ad}{c} \\ 0 & 1 \end{bmatrix},
\end{aligned}$$

which is in N, since $\frac{ad}{c} \in \mathbb{R}$ as $c \neq 0$. $(\because ac \neq 0)$, as required.
Hence N is a normal subgroup of G.

■

DAY 4
Normal subgroup (part 2)

এবার আমরা কিছু বহুল ব্যবহৃত normal subgroup-এর কথা শিখব। প্রতি ক্ষেত্রে আমরা subgroup-টা কী সেটা প্রথমে লিখব, এবং তারপর সেটা যে normal subgroup সেটা প্রমাণ করব।

4.1 Well-known examples

H যদি G-এর একটা subgroup হয় তবে H-কে normal subgroup দেখানোর একটা কায়দা হল এইটা দেখানো--

$$\forall g \in G \quad gHg^{-1} \subseteq H.$$

এটাকেই আমরা definition 3 নাম দিয়েছিলাম। বিশদ করে লিখলে হয়--

$$\forall g \in G \quad \forall h \in H \quad ghg^{-1} \in H.$$

প্রতি ক্ষেত্রে এটাই আমরা ব্যবহার করব।

4.1.1 Alternating subgroup

Example 23: Show that the alternating subgroup A_n is a normal subgroup of the symmetric group S_n.[4] **(2011.3a,2008.4a)**

SOLUTION: প্রথমে চট্ করে মনে করে নিই, A_n জিনিসটা কী ছিল--

> We know that A_n is the subgroup of S_n consisting of all the even permutations of $\{1, ..., n\}$.

যেমন, cycle notation-এ ভাবতে চাও তবে $S_3 = \{e, (1,3,2), (1,2,3), (2,3), (1,3), (1,2)\}$. এখানে even permutation-রা হল e আর যাদের cycle-এর দৈর্ঘ্য *odd*. তাই $A_3 = \{e, (1,3,2), (1,2,3)\}$.
এবার প্রমাণে হাত দিই--

> To show that A_n is a normal subgroup of S_n we have to show that
>
> $$\forall \pi \in S_n \quad \pi A_n \pi^{-1} \subseteq A_n,$$
>
> ie,
>
> $\forall \pi \in S_n \quad \forall \lambda \in A_n \quad \pi\lambda\pi^{-1} \in A_n.$
>
> $\forall \pi, \lambda$
>
> Take any $\pi \in S_n$ and any $\lambda \in A_n$.
>
> For $\mu \in S_n$, we know that μ^{-1} and μ have the same parity.
>
> <u>Case 1: parity(π) = even:</u>
>
> Then
>
> $$\begin{aligned} \text{parity}(\pi\lambda\pi^{-1}) &= \text{parity}(\pi) + \text{parity}(\lambda) + \text{parity}(\pi^{-1}) \\ &= \text{even} + \text{even} + \text{even} = \text{even}. \end{aligned}$$
>
> Hence $\pi\lambda\pi^{-1} \in A_n$, as required.
>
> <u>Case 2: parity(π) = odd:</u>
>
> Then
>
> $$\begin{aligned} \text{parity}(\pi\lambda\pi^{-1}) &= \text{parity}(\pi) + \text{parity}(\lambda) + \text{parity}(\pi^{-1}) \\ &= \text{odd} + \text{even} + \text{odd} = \text{even}. \end{aligned}$$
>
> Hence $\pi\lambda\pi^{-1} \in A_n$, as required.

■

এই অংকটা আমরা সরাসরি সংজ্ঞা ব্যবহার করে করলাম, তাই লম্বা হল। অংকটাকে একলাইনেও করে ফেলা যেত, যদি আমরা Example 18 নম্বর অংকটা লাগাতাম। সেখানে বলা ছিল যে যদি $[G : H] = 2$ হয় তবে H-টা G-এর normal

subgroup হবে। আমরা জানি যে finite group-এর ক্ষেত্রে

$$[G : H] = |G|/|H|.$$

এখানে $G = S_n$ আর $H = A_n$. আমরা জানি যে S_n-এর মধ্যে যে $n!$-টা permutation আছে, তার মধ্যে ঠিক অর্ধেক হল even. তাই $|S_n|/|A_n| = 2$. সুতরাং $[S_n : A_n] = 2$. অতএব A_n অবশ্যই S_n-এর একটা normal subgroup হবে।

4.1.2 Centre

কোনো group-এর centre বলতে কী বোঝায়, সেটা আমরা আগেই দেখেছি--সব মিশুকে element-দের set, সেই সব element যারা G-এর সবার সঙ্গে commute করে। G-এর centre-কে লেখে $Z(G)$. সংজ্ঞাটা নীচের অংকে আরেকবার মনে করিয়ে দেওয়া হয়েছে। সেই সঙ্গে এটাও বলা হয়েছে $Z(G)$ সর্বদাই G-এর একটা normal subgroup হয়।

Example 24: Let $(G, \circ)$ be a group and $Z(G) = \{x : x \circ g = g \circ x \text{ for all } g \in G\}$. Examine whether $Z(G)$ is a normal subgroup of $(G, \circ)$ or not.[4] **(2011.4a,2007.3a)**

SOLUTION: প্রথমে subgroup দেখানো থেকে শুরু করি--

> Step 1: Shall show that $Z(G)$ is a subgroup of G.

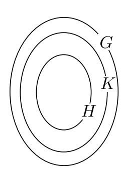
আগে nonempty দেখাই--

> $\forall g \in G$ we have $e \circ g = g \circ e$.
> So $e \in Z(G)$. Hence $Z(G) \neq \phi$.

তারপর দেখাই যে $a, b \in Z(G)$ হলে $a^{-1}b \in Z(G)$ হবে।

> Shall show
> $$\forall a, b \in Z(G) \quad a^{-1}b \in Z(G),$$
> ie,
> ◎ $\forall a, b \in Z(G) \quad \forall g \in G \quad g(a^{-1}b) = (a^{-1}b)g.$
> $\boxed{\forall a, b, g}$ Take any $a, b \in Z(G)$ and any $g \in G$.

Fig 21



Then

$$\begin{aligned} g(a^{-1}b) &= (ga^{-1})b \\ &= (ag^{-1})^{-1}b \end{aligned}$$

এখানে আমরা এই সূত্রটা লাগালাম--
$p, q \in G$ হলে $(pq)^{-1} = q^{-1}p^{-1}$ হয়।

$$\begin{aligned} &= (g^{-1}a)^{-1}b \quad [\because a \in Z(G)] \\ &= a^{-1}gb \\ &= a^{-1}bg \quad [\because b \in Z(G)]. \end{aligned}$$

এবার normal দেখাব--

Step 2: Shall show that $Z(G)$ is normal in G,

ie,

$\forall g \in G \quad \forall z \in Z(G) \quad gzg^{-1} \in Z(G).$

$\forall g, z$ Take any $g \in G$ and any $z \in Z(G)$.

Then

$$\begin{aligned} gzg^{-1} &= zgg^{-1} \quad [\because z \in Z(G), \quad \therefore gz = zg] \\ &= z \in Z(G), \end{aligned}$$

as required.

■

4.1.3 Normaliser

এবার আমরা একটু অন্যদিক থেকে আক্রমণ করব। এতক্ষণ আমরা একটা group G নিয়ে শুরু করে তার কোনো একটা normal subgroup H বার করছিলাম। এবার আমরা শুরু করব G-এর মধ্যে একটা যে কোনো subgroup H নিয়ে, সেটা normal হোক বা নাই হোক। এবার দেখব H আর G-এর মাঝামাঝি এমন কোনো subgroup K পাওয়া যায় কিনা, যাতে H-টা K-র মধ্যে normal হয়, মানে "$\forall g \in G \quad gHg^{-1} \subseteq H$ " যদি নাও হয়, অন্ততঃ যেন

$$\forall k \in K \quad kHk^{-1} \subseteq H$$

হয়। এখানে আমরা "মাঝামাঝি" বলতে $H \subseteq K \subseteq G$ বোঝাচ্ছি। Fig 21 দ্যাখো। এরকম একটা K তো আছেই, সেটা হল $K = H$ (কেন?)। প্রশ্ন হল সবচেয়ে বড় এরকম K কী আছে? সবচেয়ে বড় এরকম K-র একটা গালভরা নাম আছে--**normaliser** of H in G. একে লেখা হয় $N(H)$. এটা মোটেই ভালো notation নয়, কারণ এখানে G-এর কোনো উল্লেখ নেই, যদিও normaliser-টা অবশ্যই G-এর উপরেও নির্ভর করে।
নীচের অংকটা এই $N(H)$ নিয়েই। এখানে $N(H)$ বার করার একটা ফর্মুলা দিয়েছে।

Example 25: Let H be a subgroup of a group G and

$$N(H) = \{g \in G \mid gHg^{-1} = H\}.$$

Prove that
(i) $N(H)$ is a subgroup of G;
(ii) H is a normal subgroup of $N(H)$. [2+3] **(2013.3a,2010.4a)**
SOLUTION:

(i): Shall show that $N(H)$ is a subgroup of G.

Clearly, $eHe^{-1} = H$. So $e \in N(H)$. Hence $N(H) \neq \phi$.

Shall show

$\forall a, b \in N(H) \quad ab^{-1} \in N(H)$.

Take any $a, b \in N(H)$.

Then

$$\begin{aligned} (ab)H(ab)^{-1} &= (ab)H(b^{-1}a^{-1}) \\ &= a\big(bHb^{-1}\big)a^{-1} \quad [\text{ by associativity}] \\ &= aHa^{-1} \quad [\because b \in N(H)] \\ &= H \quad [\because a \in N(H)] \end{aligned}$$

So $ab \in N(H)$.

Thus $N(H)$ is a subgroup of G.

এবার দ্বিতীয় অংশ, যেখানে normal দেখাতে হবে--

(ii): Shall show that H is normal in $N(H)$, ie,

$\forall g \in N(H) \quad gHg^{-1} \subseteq H$.

Take any $g \in N(H)$.

Then, by definition of $N(H)$, we have $gHg^{-1} = H$.

So $gHg^{-1} \subseteq H$, as required.

■

আমরা বলেছিলাম যে, $N(H)$ হল G-এর সবচেয়ে বড় subgroup যার মধ্যে H-টা normal. এক্ষুণি যে অংকটা করলাম, তাতে কিন্তু "সবচেয়ে বড়" কথাটার প্রমাণ হল না। সেটা গুছিয়ে লিখেছি নীচের অংকটায়। চেষ্টা করে দ্যাখো।

Exercise 12: Let G be a group, and H be any subgroup of G. Let

$$N(H) = \{g \in G \mid gHg^{-1} = H\}.$$

If K is a subgroup of G such that $H \subseteq K \subseteq G$, and H is a normal in K, then show that $K \subseteq N(H)$.
HINT:
অংকটা করার আগে ঠাণ্ডা মাথায় বুঝে দ্যাখো যে, যা বলা হয়েছে সেটা আসলে সেই "সবচেয়ে বড়"-র ব্যাপারটাই।

■

এবার একটা খুব সহজ অংক দিই--

Exercise 13: যদি G-এর একটা normal subgroup হয় H, তবে $N(H)$ কি হবে? ■

4.1.4 Commutator

একধরণের group-এর বেলায় normal subgroup পাওয়া খুব সহজ--তারা হল Abelian group. কারণ এক্ষেত্রে যে কোনো subgroup-ই হল normal subgroup.
একটা group যদি Abelian নাও হয়, তবে সেটা Abelian হওয়ার থেকে "কত দূরে" আছে, সেটা মাপা যায় এইভাবে--

> যাবতীয় $a, b \in G$-এর জন্য প্রথমে $(ab)(ba)^{-1}$ বার করতে হয়। লক্ষ করো, $ab = ba$ হওয়া মানে $(ab)(ba)^{-1} = e$ হওয়া। সুতরাং $(ab)(ba)^{-1}$-জাতীয় জিনিসগুলো কত বিভিন্নরকম value নিতে পারে তার থেকে বোঝা যায় G-টা কতটা non-Abelian.

নীচের অংকটা বলছে যে, এই element-গুলোর আরেকটা অদ্ভুত গুণ আছে। এরা সবাই যদি কোনো subgroup-এর মধ্যে থাকে, তবে সেই subgroup-টা normal হতে বাধ্য! এই প্রসঙ্গে বলে রাখি যে, $(ab)(ba)^{-1}$-জাতীয় element-দের একটা নাম আছে--**commutator**.

Example 26: Let G be a group and H be a subgroup of G such that $aba^{-1}b^{-1} \in H\ \forall a, b \in G$.

Prove that H is a normal subgroup of G. **(2006)**
SOLUTION: লক্ষ করো যে, $(ab)(ba)^{-1}$-কেই এখানে $aba^{-1}b^{-1}$ লিখেছে।

Shall show that H is a normal subgroup of G, ie,

$\forall g \in G \quad \forall h \in H \quad ghg^{-1} \in H.$

$\forall g, h$ Take any $g \in G$ and any $h \in H$.

আমরা এখানে $aba^{-1}b^{-1}$-জাতীয় জিনিস নিয়ে কাজ করছি। এখানে ghg^{-1}-টা দেখতে অনেকটা এইরকমই বটে, খালি শেষে একটা h^{-1} থাকলেই হত। তাই আমরা ওটুকু জুড়ে নেব, আর একটা বাড়তি h^{-1} আনলাম বলে, সেটাকে ব্যালান্স করার জন্য একটা h-ও আনব--

Then

$$ghg^{-1} = \underbrace{ghg^{-1}h^{-1}}_{h',\ \text{say}} h.$$

Now h' is of the form $aba^{-1}b^{-1}$ and so is in H.
Hence

$$ghg^{-1} = h'h \in H,$$

as required.

■

4.2 Kernel

অংক করতে গিয়ে যতরকমভাবে normal subgroup আসে, তাদের মধ্যে নিঃসন্দেহে সবচেয়ে গুরুত্বপূর্ণ হল group homomorphism-দের kernel-রা। Kernel কী পদার্থ আশা করি মনে আছে--যদি $f : G \to G'$ একটা group homomorphism হয়, তবে

$$\ker(f) = \{x \in G \ : \ f(x) = e'\},$$

যেখানে e' হল G'-এর identity. আমরা এই অধ্যায়ের গোড়ার দিকেই দেখেছি যে, $\ker(f)$ সবসময়ে G-এর একটা subgroup হয়। নীচের অংকটা বলছে যে ব্যাপারটা আরও ভালো--শুধু subgroup নয়, kernel-রা সব সময়েই normal subgroup-ও হয়! বস্তুতঃ, ব্যাপারটা তার চেয়েও ভালো--এর converse-টাও আবার সত্যি, মানে যদি তুমি যেকোনো একটা normal subgroup নাও H, তবে এমন একটা group homomorphism পাবে $f : G \to G'$, যাতে $\ker(f) = H$ হয়! এই শেষের অংশটুকু অবশ্য আজকে প্রমাণ করব না, ওটা এই অধ্যায়ের শেষের দিনের জন্য তোলা থাক। আমরা আপাততঃ প্রথম অংশটা প্রমাণ করি--

Example 27: If f is a homomorphism of a group $(G, \circ)$ onto a group $(G', \star)$, then prove that $\ker f$ is a normal subgroup of G.[3] **(2013.4b,2011.4b,2008.3a,2006.3b)**

SOLUTION: প্রথমেই বলে রাখি যে, এখানে onto হবার কোনো দরকার নেই। যেকোনো group homomorphism হলেই একই প্রমাণ। প্রথমে দেখাব যে $\ker(f)$ একটা subgroup, যেটা আগেও দেখিয়েছি। সুতরাং সংক্ষেপে সারি।

> Let $H = \ker f$.
>
> Step I: Shall show that H is a subgroup of G.

দুটো জিনিস দেখালেই চলবে--এক, nonempty.

> $\because f(e) = e'$, $\therefore e \in \ker f$.
>
> $\therefore H \neq \phi$.

আর দুই, $a, b \in H$ হলে $a^{-1}b \in H$ হয়--

> Take any $a, b \in H$.
>
> Then, since f is a homomorphism, $f(a^{-1}b) = (f(a))^{-1}f(b) = (e')^{-1}e' = e'$.
>
> $\therefore a^{-1}b \in H$.
>
> Hence H is a subgroup of G as required.

এইবার normal দেখাব--

> Step 2: Shall show that H is a normal subgroup,
>
> ie, $\forall g \in G \quad gHg^{-1} \in H$, ie,
>
> $\forall g \in G \quad \forall h \in H \quad ghg^{-1} \in H$.
>
> $\forall g, h$ Take any $g \in G$ and any $h \in H$.
>
> Then, since f is a homomorphism,
>
> $$f(ghg^{-1}) = f(g)f(h)f(g^{-1}) = f(g)e'(f(g))^{-1} = e'.$$

So $ghg^{-1} \in \ker f = H$, as required.

■

DAY 5
Quotient group (part 1)

5.1 Normal subgroup-রা কোথা থেকে এল?

আমরা normal subgroup নিয়ে অনেক আলোচনা করলাম। কিন্তু মানুষ আদৌ প্রথমে কেন normal subgroup-এর কথা ভেবেছিল সে কথা বলি নি। এবার সেই গল্পে আসি। তার জন্য প্রথমে একটা অংক দেখি।

Example 28: দেখাও যে, এই equation-টার কোনো solution-ই integer (পূর্ণসংখ্যা) নয়--

$$x^5 + 2x^4 + 3x^3 - 37x^2 - 5x + 10395 = 0.$$

SOLUTION: এই অংকটা দেখে দুরকম কায়দা মাথায় আসতে পারে--এক, এর যাবতীয় solution বার করে দেখানো যে, কোনোটাই integer নয়। আর দুই, সব integer বসিয়ে বসিয়ে দেখানো যে, equation-টা কোনো integer-এই hold করে না (অর্থাৎ সিদ্ধ হয় না)। কিন্তু এরকম একটা বিট্‌কেল 5 degree equation-এর যাবতীয় solution তো দূরের কথা, একটা solution-ও বার করা সহজ নয়। আর integer তো আছে infinitely many, তাদের সবাইকে বসিয়ে বসিয়ে দেখতে গেলে এই জন্মে যে আর কিছুই করা হবে না! আসলে কিন্তু একটা কায়দা জানা থাকলে এই অংকটা করা খুবই সহজ।
যদি x একটা even number নিই, তবে $x^5, 2x^4, 3x^3, 37x^2$ এবং $5x$ সবাই হবে even. কারণ কোনো even সংখ্যার সঙ্গে যাই গুণ কর না কেন, গুণফল even-ই থাকে। সুতরাং--

$$\underbrace{x^5}_{\text{even}} + \underbrace{2x^4}_{\text{even}} + \underbrace{3x^3}_{\text{even}} - \underbrace{37x^2}_{\text{even}} - \underbrace{5x}_{\text{even}} + 10395 = 0.$$

আবার বিভিন্ন even সংখ্যাকে যোগ-বিয়োগ করলেও even সংখ্যাই পাওয়া যায়। অতএব--

$$\underbrace{x^5 + 2x^4 + 3x^3 - 37x^2 - 5x}_{\text{even}} + 10395 = 0.$$

কিন্তু শেষের ওই 10395-টা তো odd. আমরা জানি যে একটা even সংখ্যার সঙ্গে একটা odd সংখ্যা যোগ করলে উত্তরটা odd হয়। তার মানে

$$\underbrace{x^5 + 2x^4 + 3x^3 - 37x^2 - 5x + 10395}_{\text{odd}} = 0.$$

Fig 22

⋮	⋮	⋮	⋮
−8	−7	−6	−5
−4	−3	−2	−1
0	1	2	3
4	5	6	7
8	9	10	11
⋮	⋮	⋮	⋮

$6 + (-1) = 5$

$10 + 11 = 21$

$-10 + (-5) = -15$

Fig 23

কিন্তু সেটা তো হতে পারে না, কারণ 0 মোটেই একটা বিজোড় সংখ্যা নয়[1]। সুতরাং বুঝতেই পারছ যে, x-এর পক্ষে একটা even সংখ্যা হওয়া অসম্ভব। ভালো করে দ্যাখো যুক্তিটা স্পষ্ট হল কিনা।
এবার দেখাব যে, x একটা odd number-ও হতে পারে না। এক্ষেত্রে মনে রাখতে হবে যে, দুটো odd সংখ্যাকে গুণ করলে odd-ই থাকে, কিন্তু ওদের যোগ-বিয়োগ করলে উত্তরটা even হয়ে যায়। সুতরাং x-টা odd হলে ব্যাপারটা দাঁড়াচ্ছে এইরকম--

$$\underbrace{\underbrace{\underbrace{\underbrace{\underbrace{\underbrace{x^5}_{\text{odd}}+\underbrace{2x^4}_{\text{even}}}_{\text{odd}}+\underbrace{3x^3}_{\text{odd}}}_{\text{even}}-\underbrace{37x^2}_{\text{odd}}}_{\text{odd}}-\underbrace{5x}_{\text{odd}}}_{\text{even}}+\underbrace{10395}_{\text{odd}}}_{\text{odd}}=0.$$

সুতরাং ফের সেই সমস্যা--0 হয়ে যাচ্ছে একটা বিজোড় সংখ্যা, contradiction! সুতরাং x-টা একটা odd number-ও হতে পারে না।
সুতরাং সব মিলিয়ে দাঁড়ালো এই যে, এই equation-টার কোনো integer সমাধানই নেই। ■

এই যে কায়দাটা করলাম তাতে যেটা কাজে লাগল, সেটাকে বলা যায় জোড়-বিজোড়ের নামতা--

যোগ-বিয়োগ	গুণ
even $\pm$ even $=$ even	even $\times$ even $=$ even
even $\pm$ odd $=$ odd	even $\times$ odd $=$ even
odd $\pm$ odd $=$ even	odd $\times$ odd $=$ odd

এইগুলো আমাদের অপরিচিত নয়। যেমন, odd+odd=even দেখাতে হলে যে কোনো দুটো odd সংখ্যা নিয়ে শুরু করি-- $2m+1$ আর $2n+1$. এদের যোগ করলে হয় $2m+1+2n+1 = 2(m+n+1)$, যেটা even.
Gauss (গাউস্) নামের একজন বিখ্যাত গণিতজ্ঞ ছিলেন। তিনি এই কায়দাটাকে আরেক ধাপ এগিয়ে নিয়েছিলেন এইভাবে-- আমরা জানি, একটা সংখ্যাকে even বলে যদি সেটা 2 দিয়ে ভাগ যায়, মানে 2 দিয়ে ভাগ করলে ভাগশেষ 0 হয়। আর odd বলে যদি 2 দিয়ে ভাগ করলে ভাগশেষ 1 হয়। সুতরাং জোড়-বিজোড়ের নামতাটা হল 2 দিয়ে ভাগ করে ভাগশেষের নামতা। Gauss লক্ষ করেন যে শুধু 2 কেন, যে কোনো $m \geq 2$-এর ক্ষেত্রেই একই কাজ করা যায়। ধরো $m = 4$ নিলাম। যদি কোনো সংখ্যাকে 4 দিয়ে ভাগ করি তবে কী কী ভাগশেষ পেতে পারি? উত্তর হল--$0, 1, 2$ আর 3. তার মানে যাবতীয় integer-দের set, অর্থাৎ $\mathbb{Z}$, এখন চারটে দলে ভাগ হয়ে গেল (Fig 22)--

- 0-র দল--সেই সব সংখ্যারা যাদের 4 দিয়ে ভাগ করলে 0 ভাগশেষ থাকে (মানে যারা 4 দিয়ে ভাগ যায়)।
- 1-এর দল--সেই সব সংখ্যারা যাদের 4 দিয়ে ভাগ করলে 1 ভাগশেষ থাকে, যেমন $5, 9$, ইত্যাদি। এই দলে -3-ও আছে, কারণ -3-কে 4 দিয়ে ভাগ করলে ভাগশেষ থাকে 1, যেহেতু $-3 = 4 \times (-1) + 1$.

[1] 0 একটা even সংখ্যা, কারণ $0 = 2 \times 0$.

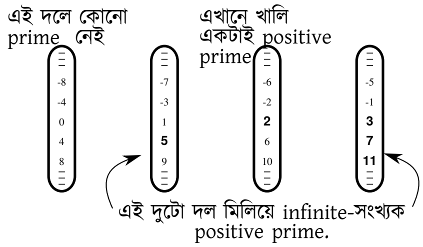


Fig 24

- 2-এর দল--সেই সব সংখ্যারা যাদের 4 দিয়ে ভাগ করলে 2 ভাগশেষ থাকে, যেমন $6, 10, -2$, ইত্যাদি।
- 3-এর দল--সেই সব সংখ্যারা যাদের 4 দিয়ে ভাগ করলে 3 ভাগশেষ থাকে, যেমন $15, 7, -13$, ইত্যাদি।

আমরা এই বইয়ে ইতিপূর্বেই coset-দের কথা শিখেছি। সুতরাং Fig 22 দেখে এই চারটে দলকে coset বলে চিনতে অসুবিধা হবার কথা নয়। আগে যেমন জোড়-বিজোড়ের নামতা দেখেছিলাম, এখানে তেমনি এই চারটে coset-এর নামতা করব। একটা উদাহরণ নিয়ে শুরু করি--ধরো 2-এর দল থেকে যে কোনো একটা সংখ্যা নিলাম, যেমন 2. আর 3-এর দল থেকে একটা সংখ্যা নিলাম, ধরো 7. দুটোকে যোগ করে পাবে $2 + 7 = 9$. সেটা রয়েছে 1-এর দলে (কারণ 9-কে 4 দিয়ে ভাগ করলে ভাগশেষ থাকে 1). মজার কথা হল এই ব্যাপারটা সব সময়েই হবে, অর্থাৎ 2-এর দলের যে কোনো সংখ্যার সঙ্গে 3-এর দলের যে কোনো সংখ্যা যোগ করলেই উত্তরটা সর্বদাই 1-এর দলে থাকতে বাধ্য। কয়েকটা উদাহরণ রয়েছে Fig 23-এ। তাই আমরা এভাবেও লিখতে পারি--

2-এর দল $+$ 3-এর দল $=$ 1-এর দল।

এমনটা কেন হচ্ছে সেটা বোঝা মোটেই কঠিন নয়। 2-এর দলের যে কোনো সংখ্যাই দেখতে $4m + 2$-এর মত, আর 3-এর দলের সদস্যদের চেহারা হল $4n + 3$-এর মত। সুতরাং যোগ করলে পাব

$$(4m + 2) + (4n + 3) = 4(m + n) + 5 = 4(m + n + 1) + 1,$$

যাকে 4 দিয়ে ভাগ করলে 1 ভাগশেষ থাকে, তাই যোগফলটা 1-এর দলে থাকবে।
একইরকম কথা বিয়োগের বেলাতেও খাটে। যেমন, 1-এর দলের যে কোনো সংখ্যার negative-দের নিয়েই 3-এর দলটা তৈরী, মানে

$-$(1-এর দল) $=$ 3-এর দল।

Exercise 14: 2-এর দলের negative কোন দল হবে? (1-এর দল) $-$ (2-এর দল) কত? ■

এবার পুরো ব্যাপারটাকে coset-এর ভাষায় লিখি। এখানে 0-র দলটা হল $\mathbb{Z}$-এর একটা subgroup, যার নাম দিলাম ধরো H. তাহলে দল চারটে হল

$$H, \quad 1 + H, \quad 2 + H, \quad 3 + H.$$

লক্ষ কর যে, 1 এবং 5 দুজনেই একই দলের মধ্যে আছে। তাই 1-এর দল আর 5-এর দল আসলে একই, মানে $1 + H = 5 + H$.
এইবার দ্যাখো যোগ-বিয়োগের নামতাটাকে কিরকম সুন্দরভাবে লিখে ফেলা যায়--

$$(m + H) + (n + H) = (m + n) + H \text{ এবং } -(m + H) = (-m) + H.$$

একই রকম জিনিস করা যায় গুণের বেলাতেও--

$$(m + H)(n + H) = (mn) + H,$$

অর্থাৎ m-এর দলের <u>যে কোনো</u> সংখ্যার সঙ্গে n-এর দলের <u>যে কোনো</u> সংখ্যা গুণ করলে গুণফলটা <u>সর্বদাই</u> mn-এর দলে গিয়ে পড়ে।

আচ্ছা, এতসব করে লাভ কী হচ্ছে? Gauss দেখেছিলেন যে এই দলাদলির কায়দা দিয়ে অনেক অংক সহজে কষে ফেলা যায়। যদিও সেই অংকগুলোই আমাদের প্রধান আলোচ্য বিষয় নয়, কিন্তু এই দলাদলি কায়দাটার ক্ষমতা সম্পর্কে একটা ধারণা দেওয়ার জন্য দুটো ছোটো উদাহরণ দেখাই। কারণ এই কায়দাটা থেকেই normal subgroup-এর জন্ম।

Example 29: ধরো n হল একটা odd, square number. খালি এইটুকুমাত্র তথ্যের ভিত্তিতে বলতে পারো 4 দিয়ে n-কে ভাগ করলে কত ভাগশেষ থাকবে?

SOLUTION: প্রথমেই একটা জিনিসের দিকে তোমার দৃষ্টি আকর্ষণ করি--$\mathbb{Z}$-কে যে চারটে দলে ভাঙা হয়েছে, তার মধ্যে 1-এর দল আর 3-এর দল তৈরী হয়েছে odd সংখ্যাদের নিয়ে। সব even সংখ্যারা পড়েছে বাকি দুটো দলে। এই কথাটা মাথায় রেখে সমাধানটা শুরু করি।

যেহেতু n একটা square number, তার মানে $n = m^2$ যেখানে m কোনো একটা integer. সুতরাং m-টা চারটে দলের কোনো একটা দলে থাকবে। এখন $n(= m^2)$ যেহেতু odd, তাই m-ও odd হতে বাধ্য। সুতরাং m আছে হয় 1-এর দলে, নয়তো 3-এর দলে। তাই $n = m^2$ থাকবে হয় $(1+H)^2 = (1^2)+H = 1+H$-এ বা $(3+H)^2 = (3^2)+H = 9+H$-এ। কিন্তু $9 + H = 1 + H$. তার মানে m যে দলেই থাক না কেন n সব সময়েই $1 + H$-এই থাকবে। সুতরাং উত্তর হল n-কে 4 দিয়ে ভাগ করলে ভাগশেষ হবে 1. ■

এবার আরেকটা উদাহরণ দেখি, যেখানে এই দলাদলির নামতা জানা না থাকলে এগোনো খুবই কঠিন। আমরা জানি যে, অসংখ্য positive prime number আছে--there are infinitely many positive primes–2,3,5,7,... ইত্যাদি। এদের মধ্যে কতগুলো করে কোন্ দলের মধ্যে পড়েছে? 0-র দলে অবশ্যই কেউ নেই, কারণ একটা prime সংখ্যা তো আর 4 দিয়ে ভাগ যেতে পারে না! 2-এর দলে আছে ঠিক একটাই positive prime– 2 স্বয়ং। সুতরাং বাকী সবাই আছে 1-এর দল আর 3-এর দলের মধ্যে। Fig 24 দ্যাখো। প্রশ্ন হল--এ দুজনের কার ভাগে কটা করে positive prime পড়েছে? এমন হতে পারে যে, দুই দলেই infinitely many করে আছে, আবার এমনও হতে পারে, একটা দলে হয়তো খালি finitely many আছে, অন্যটায় infinitely many. এই নিয়েই নীচের অংকটা। প্রথমে একটা লক্ষ করো-- 1-এর দলে সংখ্যাদের নিজেদের মধ্যে যতই গুণ কর না কেন, গুণফলটা 1-এর দলের মধ্যেই থাকে, কারণ

$$(1 + H) \times (1 + H) = (1 \times 1) + H = 1 + H.$$

এই কথাটা মাথায় রেখে নীচের অংকটা দ্যাখো।

Example 30: Show that there infinitely many primes of the form $4n + 3$.

SOLUTION: দেখাতে বলেছে যে 3-এর দলে অসংখ্য prime আছে। আমরা contradiction লাগাব। ধরো 3-এর দলে খালি finite সংখ্যক prime আছে--

$$p_1, \quad p_2 = 7, ..., p_n.$$

এরকম প্রথম prime-টা হল $p_1 = 3$, দ্বিতীয়টা হবে $p_2 = 7$, ইত্যাদি। এদের ব্যবহার করে একটা নতুন সংখ্যা বানাই--

$$N = 4p_2p_3 \cdots p_n + 3.$$

লক্ষ কর আমরা এখানে p_2 থেকে শুরু করেছি। একটু চিন্তা করলেই বুঝবে যে--

- N রয়েছে 3-এর দলে।
- N-কে p_2 দিয়ে ভাগ যায় না (3 ভাগশেষ থাকে), একইভাবে $p_3, ..., p_n$ দিয়েও ভাগ যায় না।
- আবার $p_1 = 3$ দিয়েও ভাগ যায় না, কারণ সেক্ষেত্রে p_1 দিয়ে $p_2p3_3 \cdots p_n$-কেও ভাগ যেতে হয়, যেটা অসম্ভব, কারণ p_i-রা সকলেই prime.

সুতরাং N-এর যাবতীয় prime factor-রাই এসেছে 1-এর দল থেকে। কিন্তু সেটা তো হতে পারে না, কারণ আমরা দেখেছি যে, 1-এর দলে সংখ্যাদের নিজেদের মধ্যে যতই গুণ কর না কেন, গুণফলটা 1-এর দলের মধ্যেই থাকে। কিন্তু আমাদের N তো এদিকে রয়েছে 3-এর দলে! সুতরাং contradiction! ■

এরকম আরও অনেক দলাদলির অংক বানানো যায়, এবং Gauss-এর এই কায়দাটা অংকের জগতের অন্যতম গুরুত্বপূর্ণ হাতিয়ার। এবং এই হাতিয়ারটাকে group theory-তে খাটাবার চেষ্টা করতে গিয়েই normal subgroup-এর প্রথম উদ্ভব। এবার আমরা সেটাই আলোচনা করব। সেখান থেকেই জন্ম নেয় একটা নতুন জিনিস--**quotient group**.

5.2 Quotient group কাকে বলে?

আমরা এই দলাদলির ব্যাপারটা এবার যে কোনো group-এর ক্ষেত্রেই করার চেষ্টা করব। এতক্ষণ কাজ করছিলাম $(\mathbb{Z},+)$ নিয়ে, এবার তার জায়গায় নেব যে কোনো group, যার নাম দিলাম ধরো $(G,\star)$. আমরা $(\mathbb{Z},+)$-এর মধ্যে একটা subgroup নিয়েছিলাম H. এখানে H-কে নেব $(G,\star)$-এর একটা subgroup. ওখানে কোনো $n\in\mathbb{Z}$-এর দল বলতে বুঝতাম $n+H$, এখানে কোনো $g\in G$-এর দল বলতে বুঝব $g\star H$.
ওখানে দলাদলির কায়দাটা ছিল এইরকম--

$$\forall m,n\in\mathbb{Z}\qquad (m+H)+(n+H)=(m+n)+H,$$
$$\text{এবং } \forall n\in\mathbb{Z}\qquad -(n+H)=(-n)+H.$$

সুতরাং এখানে আমরা প্রত্যাশা করব যে

$$\forall g_1,g_2\in G\qquad (g_1\star H)\star(g_2\star H)=(g_1\star g_2)\star H,$$
$$\text{এবং } \forall g\in G\qquad (g\star H)^{-1}=(g^{-1})\star H.$$

এই প্রত্যাশাদুটো সত্যিই পূর্ণ হবে কিনা দেখার আগে ভালো করে বুঝে নিই যে, এ দুটোর মানেটা কী। যখন বলছি

"$\forall g_1,g_2\in G\quad (g_1\star H)\star(g_2\star H)=(g_1\star g_2)\star H$",

তার মানে হল--যদি

- g_1-এর দল থেকে যা খুশি একটা element $\overline{g}_1$ নিই,
- g_2-র দল থেকে যা খুশি একটা element $\overline{g}_2$ নিই,

তবে আশা করছি যে

- $\overline{g}_1\star\overline{g}_2$ থাকবে $g_1\star g_2$-এর দলে।

একইভাবে যখন বলছি

Fig 25

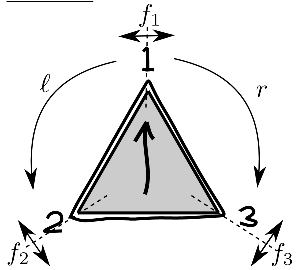
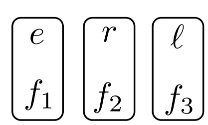


Fig 26



$$\forall g \in G \quad (g \star H)^{-1} = (g^{-1}) \star H,$$

তার অর্থ--যদি

- g-এর দল থেকে যা খুশি element $\overline{g}$ নিই,

তবে আমাদের আশা এই যে,

- $\overline{g}^{-1}$ এবং g^{-1} একই দলে থাকবে।

প্রশ্ন হল, এই প্রত্যাশাদুটো কি যে কোনো group G-এর যে কোনো subgroup H-এর ক্ষেত্রেই পূর্ণ হবে? দুঃখের কথা, এর উত্তর হল--না। কেন, সেটা বোঝা কঠিন নয়। যেমন দ্বিতীয় প্রত্যাশাটার কথাই ধরো--আমরা g-এর দল থেকে কোনো একটা element নিয়েছিলাম $\overline{g}$. মানে $\overline{g} \in g \star H$.
তাই $\overline{g}$-কে অবশ্যই এইভাবে লেখা যাবে-- $\overline{g} = g \star h$, যেখানে h হল H-এর কোনো একটা element. আমরা চাইছি যাতে $(\overline{g})^{-1}$ আর g^{-1} থাকে একই দলে, মানে $\overline{g}^{-1} \in g^{-1} \star H$ হয়। তার মানে $\overline{g}^{-1} = g^{-1} \star h'$ হবে, যেখানে $h' \in H$. অর্থাৎ $\overline{g}^{-1}$-কে ডানদিকে আর h'-কে বাঁদিকে নিয়ে গিয়ে $(h')^{-1} = \overline{g}g^{-1}$. সুতরাং শর্তটা দাঁড়াচ্ছে $\overline{g}g^{-1} \in H$. এবার যেহেতু $\overline{g} = gh$, তাই এটাকে লেখা যায়

$$ghg^{-1} \in H.$$

সুতরাং আমাদের দ্বিতীয় প্রত্যাশাটা পূর্ণ হওয়া মানে হল

$$\forall g \in G \quad \forall h \in H \quad ghg^{-1} \in H.$$

এই শর্তটা আমাদের অপরিচিত নয়। এর মানেই হল H-টা G-এর যে কোনো subgroup হলে চলবে না, একটা normal subgroup হতে হবে। মজার কথা হল, প্রথম প্রত্যাশাটার জন্য আর বাড়তি কিছু শর্ত লাগবে না, normal subgroup হলে ওই প্রত্যাশাটাও আপনাআপনিই পূর্ণ হবে! এই ব্যাপারটা group theory-তে অত্যন্ত গুরুত্বপূর্ণ, তাই পুরো জিনিসটাকে একটা theorem হিসেবে গুছিয়ে লিখে এক্ষুণি প্রমাণ করব। কিন্তু তার আগে একটা উদাহরণ দিয়ে একটু দেখে নিই যে, H যদি G-এর normal subgroup না হয়, তবে কীরকম বিপত্তি ঘটতে পারত।

Example 31: এখানে আমরা আবার $G = (S_3, \circ)$ নিয়ে কাজ করব, মানে সেই ত্রিভুজের উদাহরণ (Fig 25)। আমরা আগে দেখেছিলাম যে, এর মধ্যে $H = \{e, f_1\}$ একটা non-normal subgroup. চট্‌পট্‌ এটার left coset-গুলোকে লিখে ফেলি। Fig 26 দ্যাখো।
এবার প্রশ্ন হল প্রথম দুটো দলকে "যোগ" করলে (বা বলা উচিত $\circ$ করলে) কোন দলটা পাব? হাতে কলমে ত্রিভুজ ঘুরিয়ে করলে মজা পাবে। কিন্তু যদি সে সুবিধা না থাকে তবে doubledecker notation ব্যবহার করতে পারো--

$$r = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \ \ell = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \ f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \ f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \ f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

SOLUTION: প্রথম দলদুটো থেকে একটা করে প্রতিনিধি নেওয়া যাক। ধরো প্রথম দল থেকে নিলাম f_1 আর দ্বিতীয় দল থেকে নিলাম r. দেখতে চাই $f_1 \circ r$ কোন দলে গিয়ে পড়ে।

$$\begin{array}{c|ccc} & 1 & 2 & 3 \\ r & & & \\ & 3 & 1 & 2 \\ f_1 & & & \\ & 2 & 1 & 3 \end{array}$$

তার মানে $f_1 \circ r = f_3$, যেটা আছে তৃতীয় দলে। কিন্তু এ থেকেই কি জোর দিয়ে বলা যায় যে,

"(প্রথম দল) $\circ$ (দ্বিতীয় দল) $=$ (তৃতীয় দল)"?

উঁহু! যদি প্রথম দলদুটো থেকে অন্য কোনো প্রতিনিধি নিতাম তবে চিত্রটা অন্যরকম হবে। যেমন ধরো প্রথম দল থেকে e এবং দ্বিতীয় দল থেকে r. এবার $e \circ r = r$ কিন্তু মোটেই তৃতীয় দলে নেই! সুতরাং

"(প্রথম দল) $\circ$ (দ্বিতীয় দল) $=$ (কোন দল)?"

এই প্রশ্নটার মানেই হয় না। কারণ প্রথম দল থেকে কোনো g_1 আর দ্বিতীয় দল থেকে কোনো g_2 নিলে, $g_1 \circ g_2$ কোথায় গিয়ে পড়বে সেটা সম্পূর্ণই g_1, g_2-এর ব্যক্তিগত মর্জির উপরে নির্ভর করে, দলের উপরে নয়। তাই আমরা অংকের ভাষায় বলি

If H is not a normal subgroup of G, then operation on the cosets is not well-defined.

■

যাই হোক, subgroup-টা normal হলে এ সব কোনো সমস্যা হয় না। যদি G-এর একটা normal subgroup হয় H, তবে আমরা নিশ্চিন্তে লিখতে পারি--

$$\forall a, b \in G \qquad (aH)(bH) = (ab)H$$

তার মানে G-এর binary operation-টা থেকে আমরা coset-দের মধ্যে একটা binary operation পেলাম। G-এর ক্ষেত্রে যেমন binary operation-টার identity আছে e, তেমনি coset-দের মধ্যেও identity হল eH, কারণ

$$\forall a \in G \quad (aH)(eH) = (ae)H = aH \text{ এবং } (eH)(aH) = (ea)H = aH.$$

লক্ষ কর, eH আসলে H নিজেই, কারণ

$$eH = \{eh \ : \ h \in H\} = \{h \ : \ h \in H\} = H.$$

আরও লক্ষ কর-- aH-এর inverse হবে $a^{-1}H$, কারণ

$$(aH)(a^{-1}H) = (aa^{-1})H = eH = H \text{ এবং } (a^{-1}H)(aH) = (a^{-1}a)H = H.$$

আন্দাজ করতে পারছ হয়তো যে, H-এর coset-গুলো মিলে একটা নতুন group তৈরী হয়েছে! ব্যাপারটা আমরা $\mathbb{Z}$-এর উদাহরণ দিয়ে বুঝে নিই, যেখানে আমরা সব কিছুকে 4 দিয়ে ভাগ করে ভাগশেষ নিচ্ছিলাম। এর ফলে চারটে দলের সৃষ্টি হয়েছিল--0-র দল, 1-এর দল ইত্যাদি। এই দলগুলোকে নিজেদের মধ্যে যোগ বিয়োগ করা যায় (গুণও করা যায়, তবে আমরা আপাততঃ তা নিয়ে মাথা ঘামাচ্ছি না)। এর ফলে এই দলগুলো দিয়ে একটা নতুন group-এর জন্ম হয়, যাকে বলে $\mathbb{Z}_4$. এর পরিচয় আমরা এই বইতে আগেই পেয়েছি। তখন আমরা $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ লিখতাম। আর binary operation-টাকে লিখতাম $\oplus$. এইভাবে প্রকাশ করলে

"2-এর দলের কারুর সঙ্গে 3-এর দলের কাউকে যোগ করলে যোগফলটা 1-এর দলে গিয়ে পড়ে"

এই কথাটা সংক্ষেপে দাঁড়ায়--

$$2 \oplus 3 = 1.$$

এই রকম ব্যাপার যে কোনো group G-এর যে কোনো normal subgroup H-এর বেলাতেও খাটে, অর্থাৎ G-এর মধ্যে H-এর coset-গুলো মিলে একটা নতুন group-এর জন্ম দেয়। এই নতুন group-টাকে বলে একটা **quotient group** বা **factor group**. লেখার সময়ে লিখি G/H.
এই কথাটা বিভিন্নভাবে বাংলায় আলোচনা করলাম, এবার অংকের ভাষায় প্রমাণ করা যাক।

THEOREM

Let G be any group. Let H be any normal subgroup of G. Let G/H be the set of all (left) cosets of H in G, *i.e.*,

$$G/H = \{gH \;:\; g \in G\}.$$

Then

1. the binary operation
$$(g_1H) \circ (g_2H) = (g_1g_2)H$$
is well-defined on G/H.
2. $(G/H, \circ)$ is a group.

Proof: এখানে আমরা left coset লিখেছি বটে, কিন্তু normal subgroup-দের বেলায় left আর right coset-রা একই জিনিস (সেটাই ছিল normal subgroup-এর প্রথম সংজ্ঞা)। সেই জন্যই left শব্দটাকে ব্র্যাকেটের মধ্যে রেখেছি।

First part: To show

$$\forall g_1, g_2, \overline{g}_1, \overline{g}_2 \in G \quad \big(\overline{g}_1H = g_1H, \overline{g}_2H = g_2H \implies \overline{g}_1\overline{g}_2H = g_1g_2H\big).$$

এই জিনিসটার মানে হল--g_1-এর দল আর g_2-র দলকে binary operation মেলালে কী হয়, সেটা কেবল দলের উপরেই নির্ভর করে, দলের কোন প্রতিনিধি নেওয়া হচ্ছে তার ব্যক্তিগত মর্জির উপরে নয়।

$\forall g_1, g_2, \overline{g}_1, \overline{g}_2$

Take any $g_1, g_2, \overline{g}_1, \overline{g}_2 \in G$ such that

$$\overline{g}_1H = g_1H \text{ and } \overline{g}_2H = g_2H.$$

So

$$\overline{g}_1(g_1)^{-1} \in H \text{ and } \overline{g}_2(g_2)^{-1} \in H.$$

To show

$$\overline{g}_1\overline{g}_2H = g_1g_2H,$$

ie,

$$\overline{g}_1\overline{g}_2(g_1g_2)^{-1} \in H,$$

ie,

$$\overline{g}_1\overline{g}_2(g_2)^{-1}(g_1)^{-1} \in H.$$

Let $h = \overline{g}_2(g_2)^{-1}$, which is in H.
So

$$\begin{aligned} g_1\overline{g}_2(g_2)^{-1}(g_1)^{-1} &= g_1hg_1^{-1} \\ &\in H, \quad [\because H \text{ is normal}] \end{aligned}$$

as required.

এবার দ্বিতীয় অংশে আমরা group প্রমাণ করব। এখানে আমরা একেবারে group-এর সংজ্ঞার শর্তগুলো ধরে ধরে প্রমাণ করব, তাই একটু লম্বা হবে। কিন্তু এতক্ষণ যা যা আলোচনা করেছি, তার বাইরে কিছুই নেই।

Second part: Shall show that $(G/H, \circ)$ is a group.

Closure property: To show

$\forall x, y \in G/H \quad x \circ y \in G/H.$

$\forall x, y$ Take any $x, y \in G/H$.

Then $x = aH$ and $y = bH$ for some $a, b \in G$.

So

$$x \circ y = (aH) \circ (bH) = (ab)H \in G/H,$$

as required, since $ab \in G$.

Associativity: To show

$\forall x, y, z \in G/H \quad (x \circ y) \circ z = x \circ (y \circ z).$

$\forall x, y, z$ Take any $x, y, z \in G/H$.

Then $x = aH, \quad y = bH$ and $z = cH$ for some $a, b, c \in G$.

So

$$\begin{aligned}(x \circ y) \circ z &= ((aH) \circ (bH)) \circ cH \\ &= ((ab)H) \circ (cH) \\ &= ((ab)c)H \\ &= (a(bc))H \quad [\text{ by associativity of } G] \\ &= (aH) \circ (bc)H \\ &= (aH) \circ (bH \circ cH) \\ &= x \circ (y \circ z),\end{aligned}$$

as required.

Existence of identity:

Shall show that $eH = H$ is identity element of G/H where e is the identity of G,

ie,

$\forall x \in G/H \quad x \circ eH = eH \circ x = x.$

$\forall x$ Take any $x \in G/H$.

Then $x = aH$ for some $a \in G$.

So
$$(x \circ eH) = aH \circ eH = (ae)H = aH = x,$$
and
$$(eH \circ x) = eH \circ aH = (ea)H = aH = x,$$
as required.

Existence of inverse:

Shall show

$\forall x \in G/H \quad \exists y \in G/H \quad x \circ y = y \circ x = eH.$

$\forall x$ Take any $x \in G/H$.

Then $x = aH$ for some $a \in G$.

Then $a^{-1} \in G$ and so $a^{-1}H \in G/H$.

$\exists y$ Choose $y = a^{-1}H \in G/H$.

So
$$(x \circ y) = aH \circ a^{-1}H = (aa^{-1})H = eH = H,$$
and
$$(y \circ x) = a^{-1}H \circ aH = (a^{-1}a)H = eH = H,$$
as required.

[Q.E.D]

DAY 6
Quotient group (part 2)

গতকাল শিখেছি quotient group কাকে বলে। প্রথমে একটা group G আর তার একটা normal subgroup H নিয়ে শুরু করতে হয়। এবার H-এর যত coset আছে তাদের set-টা দিয়েই G/H তৈরী। এখানে আমরা left coset নিয়ে কাজ করছি, নাকি right coset নিয়ে? উত্তর হল--তাতে কিচ্ছু এসে যায় না, যেহেতু H একটা normal subgroup, তাই যেকোনো $g \in G$-এর জন্যই $gH = Hg$, মানে ওর left আর right coset-রা একই জিনিস। এবার একটা উদাহরণ নিই।

Example 32: ধরো G-এর সাইজ হল 12, আর H-এর সাইজ হল 4. তাহলে G/H-এর সাইজ কত হবে?

SOLUTION: H-এর coset-গুলো G-এর মধ্যে পাঁউরুটির স্লাইসের মত সাজানো আছে, এবং ওদের সবার সাইজই 4. সুতরাং বুঝতেই পারছ মোট coset-এর সংখ্যা $12/4 = 3$. তাই G/H-এর সাইজ 3. এই সংখ্যাটারই আরেকটা নাম হল index of H in G, যাকে লেখে $[G : H]$. ■

এই অংকটা বুঝতে পারলে নীচের ছোট্টো theorem-টা বুঝতেও অসুবিধা হবার কথা নয়--

THEOREM

Let G be any *finite* group with a normal subgroup H. Then

$$|G/H| = |G|/|H|.$$

এবার তবে আলোচনা করি quotient group শিখে লাভটা কী। এটা যে কি ভীষণ কাজের জিনিস, সেটা এক কথায় বোঝানোই কঠিন। মোটামুটিভাবে ধারণাটা এইরকম-- G/H হল G-এরই একটা সংক্ষিপ্ত সংস্করণ। একটা subgroup যে অর্থে group-এর ছোটো অংশ সে অর্থে নয়, একটা subgroup হল খালি একটা অংশমাত্র, আর quotient group হল যেন group-টাকে ফোল্ডিং ছাতার মত গুটিয়ে আনা হয়েছে। তাতে মূল group-টার কিছু বৈশিষ্ট্য চোখের আড়ালে চলে গেছে, কিন্তু বাকি বৈশিষ্ট্যগুলো সম্পূর্ণই রয়েছে। মূল group-টা যদি হয় একটা বড় গাছ, তবে subgroup হল যেন তার একটা ডাল, আর quotient group হল পুরো গাছটার বন্সাই। তাই একটা quotient group থেকে মূল group-এর বিষয়ে যতটা ধারণা করা যায়, খালি subgroup থেকে ততটা হয় না।
সেই কারণে যখন কোনো খটোমটো group G-এর খোঁজ মেলে, অমনি পণ্ডিতেরা ভারী ব্যস্ত হয়ে ওঠেন তার একটা যুৎসই normal subgroup N পেতে, তাহলে G-কে খানিকটা গুটিয়ে G/N পাওয়া যাবে। সেইটাকে পরীক্ষা করে দেখা অনেক সময়েই G-কে সরাসরি পরীক্ষা করে দেখার চেয়ে সহজতর হয়।
G-র অনেক ভালো ভালো গুণ G/N-এর মধ্যে বর্তায়, আবার কায়দা করে N নিতে পারলে G-এর বাজে বৈশিষ্ট্যগুলো G/N অব্দি পৌঁছতে পারে না। প্রথমে দেখি ভালো ভালো গুণ কীরকমভাবে G থেকে G/N-এ চলে যায়। যেমন ধরো cyclic হওয়া। এটা একটা ভালো গুণ, কারণ cyclic group-দের নিয়ে কাজ করা সহজ। G যদি cyclic হয়, তবে G/N-ও তাই হবে। এটা নিয়েই নীচের অংকটা।

Example 33: Let G be a group and N a normal subgroup of G. If G is cyclic then prove that the quotient group G/N is also cyclic. Is the converse true? Justify.[4] **(2010,2015)**

SOLUTION:

> <u>First part:</u> Let G be a cyclic group generated by c. Let N be any (normal) subgroup of G.

এখানে normal শব্দটা ব্র্যাকেটের মধ্যে লিখেছি, কারণ G যেহেতু cyclic, তাই Abelian-ও বটে। আর Abelian group-এর বেলায় যেকোনো subgroup-ই normal হতে বাধ্য, তাই normal কথাটা এখানে বলাই বাহুল্য।

> We shall show that G/N is a cyclic group generated by cN,

আমাদের দেখাতে বলেছে যে, G/N হল cyclic, তার মানে কোনো একটা element-এর বিভিন্ন power দিয়ে তৈরী। আমরা জানি যে, G/N-এর element-গুলো হল N-এর coset-রা, যাদের দেখতে gN-এর মত, যেখানে $g \in G$. সুতরাং $\because c \in G$, $\therefore cN \in G/N$. আমরা দাবী করছি যে, G/N-টা এই cN দিয়েই generated, মানে G/N-এর সব element-ই cN-এর কোনো না কোনো power–

> ie,
>
> ◎ $\forall x \in G/N \quad \exists n \in \mathbb{Z} \quad x = (cN)^n.$
>
> $\boxed{\forall x}$ Take any $x \in G/N$.
>
> Then $x = gN$ for some $g \in G$.
>
> Since G is generated by c,

$\therefore \exists n \in \mathbb{Z} \quad g = c^n$.

$\exists n$ Choose this $n \in \mathbb{Z}$.

Then

$$x = gN = c^n N = (cN)^n,$$

by definition of quotient group, as required.

আগেই বলেছি যে G থেকে G/N তৈরী করার সময়ে কায়দা করে N নিলে পরে G-এর অনেক বদ্‌গুণ G/N অব্দি পৌঁছতে পারে না। তাই G-এর থেকে G/N-এর আচরণ অনেক সময়ে বেশী ভালো হয়। ফলে G/N-এর কোনো সুবিধাজনক বৈশিষ্ট্য থাকলেই জোর দিয়ে বলা যায় না যে, G-এরও সেই বৈশিষ্ট্যটা ছিল। সেটা নিয়েই এই অংকের দ্বিতীয় অংশ--

Second part: The converse is: If G/N is cyclic, then G must be cyclic.

No, this converse is not true.

Counterexample: $N = A_3$ is a normal subgroup of $G = S_3$. We know $G/N = S_3/A_3$ is a group of size 2, which is a prime. So G/N is cyclic. But we know that $G = S_3$ is not cyclic, because it is not even Abelian.

■

Exercise 15: আমরা এক্ষুণি S_3 দিয়ে একটা counterexample দিলাম। Klein's 4-group দিয়েও দেওয়া যেত। কীভাবে? ■

এবার একটা ঠকানো অংক দিই। অতি সহজ বোকাবোকা উত্তর।

Exercise 16: Show that for any group G, there is a normal subgroup N such that G/N is cyclic. ■

আমরা দেখলাম, cyclic হওয়া এমন একটা গুণ যেটা G থেকে G/N-এ সংক্রামিত হয়। এবার দেখব যে Abelian হওয়ার ব্যাপারটাও একই রকম।

Example 34: Prove that the quotient group of a group G by a normal subgroup of it is commutative if G is commutative. Establish that the converse is not true.[4] **(2009.3a)**

SOLUTION:

First part: Let N be a normal subgroup of G.

To show G/N is commutative,

ie,

$$\forall x, y \in G/N \quad xy = yx.$$

$\forall x, y$ Take any $x, y \in G/N$.

Then $x = aN$ and $y = bN$ for some $a, b \in G$.

Then

$$(aN)(bN) = (ab)N \text{ and } (bN)(aN) = (ba)N.$$

Since G is Abelian, $ab = ba$. So, by the definition of quotient group,

$$xy = (aN)(bN) = (ab)N = (ba)N = (bN)(aN) = yx,$$

as required.

Cyclic-এর অংকটার মত এক্ষেত্রেও converse-টা নাও খাটতে পারে। প্রথমে converse-টা লিখে নিই--

Second part: The converse is: If G/N is Abelian, then G must be Abelian.
This converse is not true.
Counterexample: $N = A_3$ is a normal subgroup of $G = S_3$. We know $G/N = S_3/A_3$ is a group of size 2, which is a prime. So G/N is cyclic, and hence Abelian.
But we know that $G = S_3$ is not Abelian.

■

আমরা আগেই বলেছি যে, N-টাকে যুৎসই ভাবে নিতে পারলে এমন G/N পাওয়া সম্ভব, যার মধ্যে G-এর ভালো বৈশিষ্ট্যগুলো বজায় থাকে, অথচ খারাপ কিছু বৈশিষ্ট্য বাদ যায়। এবার তার আরও একটা উদাহরণ দেখব। ধরো G হল non-Abelian. আমরা এমনভাবে N নেব, যাতে G-টা গুটিয়ে G/N হবার সময়ে non-Abelian হওয়ার দোষটা কেটে যায়। তার একটা কায়দা বলা আছে নীচের অংকটায়।

Example 35: Let G be a group and H be a subgroup of G such that $aba^{-1}b^{-1} \in H$ $\forall a, b \in G$.

Prove that H is a normal subgroup of G and the quotient group G/H is commutative.[4] **(2006.4a)**

SOLUTION: প্রথম অংশটা আমরা আগেই করেছি Example 26-এ, commutator নিয়ে আলোচনা করার সময়ে। সুতরাং এখন খালি দ্বিতীয় অংশটুকু করব।

Second part: Shall show that G/H is Abelian, ie,

$\forall a, b \in G \quad (aH)(bH) = (bH)(aH)$.

$\forall a, b$

Take any $a, b \in G$.

Then $(aH)(bH) = (ab)H$.
Let $h = aba^{-1}b^{-1}$.
So $hba = ab$.
Also, by the given condition, $h \in H$.

Hence

$$\begin{aligned}(ab)H &= (hba)H = (hH)(ba)H = H(ba)H \\ &= (ba)H \quad [\because H \text{ is the identity of } G/H] \\ &= (bH)(aH),\end{aligned}$$

as required.

■

6.1 Isomorphism theorem

Isomorphism কাকে বলে সেটা আমরা এই অধ্যায়ের গোড়াতেই দেখেছি। Isomorphism নিয়ে বিভিন্ন গুরুত্বপূর্ণ theorem আছে, তার মধ্যে একটা আমরা শিখব। নীচের অংকটা দিয়েছি তার আগে একটু গা গরম করে নেওয়ার জন্য।

Example 36: Let H be a normal subgroup of a group G. Prove that the mapping $\theta : G \to G/H$ defined by $\theta(x) = xH$, $x \in G$ is an onto homomorphism with kernel H.[4] **(2013.4c)**

SOLUTION: প্রথমে দেখাই যে θ হল well defined, অর্থাৎ $x \in G$ হলে $\theta(x)$-টা G/H-এর মধ্যেই থাকে।

Step 1: G/H consists of all the cosets of H in G. (Since H is normal, left and right cosets are the same.) For each $x \in G$ we have $\theta(x) = xH$, a coset of H in G. So $\theta(x) \in G/H$.
Hence $\theta : G \to G/H$ is well-defined.

এবার θ-কে একটা homomorphism দেখাব--

Step 2: Shall show

$\forall x, y \in G \quad \theta(xy) = \theta(x)\theta(y).$

$\forall x, y$ Take any $x, y \in G$.

Then

$$\theta(xy) = (xy)H = (xH)(yH) = \theta(x)\theta(y),$$

by the definition of binary operation in G/H, as required.

এবার onto দেখানোর পালা--

Step 3: Shall show that $\theta : G \to G/H$ is onto, ie,

$\forall a \in G/H \quad \exists x \in G \quad \theta(x) = a.$

$\forall a$ Take any $a \in G/H$.

By definition of G/H, we have $a = xH$ for some $x \in G$.

$\exists x$ Choose this $x \in G$.

Then $\theta(x) = xH = a$, as required.

এবার দেখাব $\ker(\theta) = H$. এখানে $\ker(\theta)$ হল সেই সব $x \in G$-এর set, যাদের জন্য $\theta(x) = H$ হয়।
দুটো set-কে সমান দেখাতে হবে। তার অমোঘ পদ্ধতি তো জানিই--একবার $\ker(\theta) \subseteq H$ দেখাব, তারপর $H \subseteq \ker(\theta)$.

Step 4: Shall show that $\ker(\theta) = H$.
Take any $x \in \ker(\theta)$.
Since the identity element of G/H is H,
hence $\theta(x) = H$,
ie, $xH = H$.
$\because e \in H$, $\therefore xe \in H$, ie, $x \in H$.
$\therefore \ker(\theta) \subseteq H$.
Conversely, take any $y \in H$. Then $\theta(y) = yH = H$ by closure property of H.
So $y \in \ker(\theta)$.
$\therefore H \subseteq \ker(\theta)$.
Hence $\ker(\theta) = H$, as required.

■

এইবার আমরা isomorphism নিয়ে একটা অত্যন্ত গুরুত্বপূর্ণ theorem শিখব--

First isomorphism theorem

Let G, G' be two groups and $\Phi : G \to G'$ be a homomorphism. Let $H = \ker \Phi$. Then

1. $\Phi(G)$ is a subgroup of G'.
2. H is a normal subgroup of G.
3. G/H is isomorphic to $\Phi(G)$.

এর প্রথম দুটো অংশ আমরা এই অধ্যায়ে আগেই প্রমাণ করেছি। মনে রেখো, $\Phi(G)$ মানে এখানে Φ-এর image.
তৃতীয় অংশটা প্রমাণ করার আগে লক্ষ কর যে Φ যদি onto হয়, তবে $\Phi(G) = G'$ হবে। সুতরাং সেক্ষেত্রে তৃতীয় অংশটা বলছে G/H আর G' হল পরস্পরের সঙ্গে isomorphic, বা যাকে চিহ্ন দিয়ে লেখা হয়--$G/H \cong G'$. এটাই প্রমাণ করতে দিয়েছে নীচের অংকে। একবার নীচের অংকের সমাধানটা বুঝে গেলে theorem-টা প্রমাণ করা খুবই সোজা।

Example 37: Let G, G' be two groups and $\Phi : G \to G'$ be an onto homomorphism. Let $H = \ker \Phi$. Prove that the quotient group $G/H \cong G'$.[4] **(2012.4a)**

SOLUTION:

Consider the function $f : G/H \to G'$ defined by

$$f(gH) = \Phi(g).$$

প্রথমেই অবশ্য দেখিয়ে নিতে হবে যে, এভাবে সত্যিই একটা function তৈরী হয়, মানে well defined হয়। তার জন্য দেখাতে হবে, $g_1H = g_2H$ হলে $\Phi(g_1) = \Phi(g_2)$ হবে, নইলে আবার $g_1H = g_2H$ থেকে দুটো তীর বেরিয়ে যাবে, ফলে f আর একটা function থাকবে না।

Step 1: Shall show that

$$\forall g_1, g_2 \in G \quad \big(g_1H = g_2H \implies \Phi(g_1) = \Phi(g_2)\big).$$

$\forall g_1, g_2$ Take any $g_1, g_2 \in G$ with $g_1H = g_2H$.

Hence $g_1 \in g_2H$.

যেহেতু g_1 অবশ্যই g_1H-এর মধ্যে আছে।

$\therefore g_1 = g_2h$ for some $h \in H$.

$$\begin{aligned} \therefore \Phi(g_1) &= \Phi(g_2h) \\ &= \Phi(g_2)\Phi(h) \quad [\because \Phi \text{ is a homomorphism}] \\ &= \Phi(g_2)e' \quad [\because h \in \ker(\Phi)] \\ &= \Phi(g_2), \end{aligned}$$

as required, where $e' \in G'$ is the identity.

এবার দেখাব যে f একটা homomorphism--

Step 2: Shall show that f is a group homomorphism. ie,

$$\forall x_1, x_2 \in G/H \quad f(x_1x_2) = f(x_1)f(x_2).$$

$\forall x_1, x_2$ Take any $x_1, x_2 \in G/H$.

Then $x_1 = g_1H$ and $x_2 = g_2H$ for some $g_1, g_2 \in G$.

$$\begin{aligned} f(xy) &= f\big((g_1H)(g_2H)\big) \\ &= f((g_1g_2)H) \quad \Big[\text{by defn of quotient group}\Big] \\ &= \Phi(g_1g_2) \quad [\text{by defn of } f] \\ &= \Phi(g_1)\Phi(g_2) \quad [\because \Phi \text{ is homomorphism}] \\ &= f(g_1H)f(g_2H) \quad [\text{by defn of } f] \\ &= f(x)f(y), \end{aligned}$$

as required.

এবার দেখাতে হবে যে f হল একটা bijection. প্রথমে onto দেখাই--

Step 3: Shall show that f is onto, ie,

$\forall g' \in G' \quad \exists g \in G \quad f(gH) = g'$.

$\forall g'$ Take any $g' \in G$.

$\because \Phi$ is onto, $\therefore \exists g \in G \quad \Phi(g) = g'$.

$\exists g$ Choose this $g \in G$.

Then

$$f(gH) = \Phi(g) = g',$$

as required.

তারপর one-one–

Step 4: Shall show that f is one-one.

Enough to show that $\ker f = \{H\}$.

এটা দেখানোই যথেষ্ট কারণ $\{H\}$ হল G/H-এর identity. সুতরাং $\ker f$-এর মধ্যে যদি খালি identity ছাড়া আর কিছু না থাকে, তবে আমরা জানি যে f-টা one-one হতে বাধ্য।

Clearly, $H \in \ker f$.

⟦ Because:

$\because f(H) = f(eH) = \Phi(e) = e'$.

⟧

সুতরাং দেখানো হয়ে গেল যে $\{H\} \subseteq \ker f$. এবার দেখাব $\ker f \subseteq \{H\}$.

Let $gH \in \ker f$.

Then $f(gH) = e'$, ie, $\Phi(g) = e'$.

Hence $g \in \ker \Phi = H$.

So $gH = H \in \{H\}$.

$\therefore \ker f = \{H\}$, as required.

■

Exercise 17: If f is a homomorphism of a group $(G, \bullet)$ onto a group $(G_1, \star)$, prove that the quotient group $G/\ker f$ is isomorphic to $(G_1, \star)$.[5] **(2007.3b)**

HINT:

আগের অংকটাই। ■

এবার দুটো অংক দিই যেগুলোর উত্তর খুবই সংক্ষিপ্ত, কিন্তু সামান্য একটু মাথা খাটাতে হবে।

Exercise 18: Show that there cannot be any onto homomorphism from $\mathbb{Z}_6$ to $\mathbb{Z}_4$. ■

Exercise 19: How many different homomorphisms are possible from G to H if G is a group of order 6 and H is a group of order 35? ■

Answers

1. জলের molecule-এর group-এর সঙ্গে তুলনা করো। যদি e-র জায়গায় $(0,0)$ নাও, আর r, s_1, s_2-এর জায়গায় যথাক্রমে $(1,1),(0,1),(1,0)$ নাও, তবেই দেখবে নামটার টেবিল দুটো মিলে যাচ্ছে। **2.** ϕ-এর জায়গায় e বসাতেই হবে, বাকিগুলোকে যেভাবে খুশী। **3.** **(1)** না, $\mathbb{Z}_4$-এ $o(1)=4$, কিন্তু K_4-এ কোনো element নেই যার order=4. **(2)** না, সাইজ অসমান। **(3)** হ্যাঁ, $f(n)=2n$ একটা isomorphism. **4.** $\{0,1\}$. **5.** $\{0,3\}$. **6.** $\mathbb{Q}$ হল countable কিন্তু $\mathbb{R}$ হল uncountable, সুতরাং ওদের cardinality-ই আলাদা, অতএব $\mathbb{Q}$ এবং $\mathbb{R}$-এর মধ্যে কোনো bijection থাকাই অসম্ভব, isomorphism তো অনেক পরের কথা। **7.** $\mathbb{C}\setminus\{0\}$-এর যে কোনো element-এরই square root আছে, কিন্তু $\mathbb{R}\setminus\{0\}$-এর ক্ষেত্রে সেটা ঠিক নয়। **10.** না, $\mathbb{Z}_4$ আর K_4-এর কথা ভাবো। **11.** $h = gh'g^{-1} \in gHg^{-1}$. **12.** যদি H-টা K-র মধ্যে normal হয়, তবে যেকোনো $k \in K$ নিলেই $kHk^{-1} = H$ হবে। কিন্তু এইরকম যাবতীয় k নিয়েই তো $N(H)$ তৈরী। সুতরাং $k \in H$ হবে। তাই $K \subseteq H$ হতে বাধ্য। **13.** $N(H) = G$. **14.** 2-এর দল নিজেই। 3-এর দল। **15.** $G = \mathscr{P}(\{0,1\},\Delta)$ আর $N = \{\phi, \{0\}\}$. **16.** $N = G$ নাও। তাহলে G/N হল trivial, তাই cyclic. **18.** যদি $f:\mathbb{Z}_6 \to \mathbb{Z}_4$ সত্যিই একটা onto homomorphism হত, তবে $\mathbb{Z}_4 \cong \mathbb{Z}_6/\ker(f)$ হত। তার মানে $|\mathbb{Z}_4| \times |\ker(f)| = |\mathbb{Z}_6|$ হত। কিন্তু তার মানে হয়ে যাচ্ছে যে, 4 দিয়ে 6-কে ভাগ যায়! **19.** যদি $f: G \to H$ একটা homomorphism হয়, তবে $f(G)$ হবে H-এর একটা subgroup. তাই $|f(G)|$ দিয়ে $|H| = 35$-কে ভাগ যেতে হবে। সুতরাং $|f(G)| = 1, 5, 7$ বা 35. আবার isomorphism theorem-এর দরুণ $|f(G)|$ দিয়ে $|G| = 6$-কেও ভাগ যেতে হবে। সুতরাং একটাই সম্ভাবনা পড়ে রইল, $|f(G)| = 1$. তাই একটাই এরকম homomorphism আছে-- $\forall x \in G \quad f(x) = e_H$.

Index